

Y 4.AR 5/2 A:2003-2004/5

National Defense Authorization

NATIONAL DEFENSE AUTHORIZATION ACT  
FOR FISCAL YEAR 2004—H.R. 1588

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED  
PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES SUBCOMMITTEE HEARINGS

ON

**TITLE I—PROCUREMENT**  
**TITLE II—RESEARCH, DEVELOPMENT,**  
**TEST, AND EVALUATION**  
**TITLE III—OPERATION AND**  
**MAINTENANCE**

HEARINGS HELD

MARCH 13, 19, 27, APRIL 1, and 3, 2003



SUPERINTENDENT OF DOCUMENTS  
DEPOSITORY

JAN 12 2005

BOSTON PUBLIC LIBRARY  
GOVERNMENT DOCUMENTS DEPT





HEARING  
ON  
NATIONAL DEFENSE AUTHORIZATION ACT  
FOR FISCAL YEAR 2004—H.R. 1588

AND  
OVERSIGHT OF PREVIOUSLY AUTHORIZED  
PROGRAMS

BEFORE THE  
COMMITTEE ON ARMED SERVICES  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED EIGHTH CONGRESS  
FIRST SESSION

---

TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES SUBCOMMITTEE HEARINGS

ON  
**TITLE I—PROCUREMENT**  
**TITLE II—RESEARCH, DEVELOPMENT,**  
**TEST, AND EVALUATION**  
**TITLE III—OPERATION AND**  
**MAINTENANCE**

---

HEARINGS HELD  
MARCH 13, 19, 27, APRIL 1, and 3, 2003



---

U.S. GOVERNMENT PRINTING OFFICE

87-892

WASHINGTON : 2004

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES  
SUBCOMMITTEE

JIM SAXTON, New Jersey, *Chairman*

JOE WILSON, South Carolina  
FRANK A. LOBIONDO, New Jersey  
JOHN KLINE, Minnesota  
JEFF MILLER, Florida  
ROSCOE G. BARTLETT, Maryland  
MAC THORNBERRY, Texas  
JIM GIBBONS, Nevada  
ROBIN HAYES, North Carolina  
JO ANN DAVIS, Virginia  
W. TODD AKIN, Missouri  
JOEL HEFLEY, Colorado

MARTY MEEHAN, Massachusetts  
JIM TURNER, Texas  
ADAM SMITH, Washington  
MIKE MCINTYRE, North Carolina  
CIRO D. RODRIGUEZ, Texas  
BARON P. HILL, Indiana  
SUSAN A. DAVIS, California  
JAMES R. LANGEVIN, Rhode Island  
RICK LARSEN, Washington  
JIM COOPER, Tennessee

THOMAS HAWLEY, *Professional Staff Member*  
JEAN REED, *Professional Staff Member*  
WILLIAM NATTER, *Professional Staff Member*  
CURTIS FLOOD, *Staff Assistant*

# CONTENTS

## CHRONOLOGICAL LIST OF HEARINGS

2003

### HEARINGS:

	Page
Thursday, March 13, 2003, Fiscal Year 2004 National Defense Authorization Act—Force Protection Policy: The Role of the Department of Defense and the National Guard in Homeland Security .....	1
Wednesday, March 19, 2003, Fiscal Year 2004 National Defense Authorization Act—Department of Defense Efforts to Address The Chemical and Biological Threat .....	99
Thursday, March 27, 2003, Fiscal Year 2004 National Defense Authorization Act—Defense Science and Technology Policy and Programs .....	169
Tuesday, April 1, 2003, Fiscal Year 2004 National Defense Authorization Act—United States Special Operations Command Budget Request .....	295
Thursday, April 3, 2003, Fiscal Year 2004 National Defense Authorization Act—Department of Defense's Information Technology Programs and Policies .....	371

### APPENDIXES:

Thursday, March 13, 2003 .....	43
Wednesday, March 19, 2003 .....	127
Thursday, March 27, 2003 .....	213
Tuesday, April 1, 2003 .....	327
Thursday, April 3, 2003 .....	411

## THURSDAY, MARCH 13, 2003

### FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT— FORCE PROTECTION POLICY: THE ROLE OF THE DEPARTMENT OF DEFENSE AND THE NATIONAL GUARD IN HOMELAND SECURITY

#### STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Meehan, Hon. Martin T., a Representative from Massachusetts, Ranking Member, Terrorism, Unconventional Threats and Capabilities Subcommittee .....	2
Saxton, Hon. Jim, a Representative from New Jersey, Chairman, Terrorism, Unconventional Threats and Capabilities Subcommittee .....	1

#### WITNESSES

Lowenberg, Maj. Gen. Timothy, The Adjutant General, Director, Washington Military Department, and Chair of the Homeland Security Adjutants General Association of the United States .....	28
McHale, Hon. Paul, Assistant Secretary of Defense for Homeland Defense .....	4
Rees, Maj. Gen. Raymond, Acting Chief of the National Guard Bureau .....	26

#### APPENDIX

#### PREPARED STATEMENTS:

Lowenberg, Maj. Gen. Timothy .....	72
McHale, Secretary Paul .....	52



## PREPARED STATEMENTS—CONTINUED

Rees, Maj. Gen. Raymond .....	63
Saxton, Hon. Jim .....	47

## DOCUMENTS SUBMITTED FOR THE RECORD:

[There were no Documents submitted.]

## QUESTIONS AND ANSWERS SUBMITTED FOR THE RECORD:

Ms. Davis (Susan) .....	98
Mr. Meehan .....	97

---

**WEDNESDAY, MARCH 19, 2003**
**FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT—DEPARTMENT OF DEFENSE EFFORTS TO ADDRESS THE CHEMICAL AND BIOLOGICAL THREAT**

## STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Meehan, Hon. Martin T., a Representative from Massachusetts, Ranking Member, Terrorism, Unconventional Threats and Capabilities Subcommittee .....	100
Saxton, Hon. Jim, a Representative from New Jersey, Chairman, Terrorism, Unconventional Threats and Capabilities Subcommittee .....	99

## WITNESSES

Goldfein, Brig. Gen. Stephen, USAF, Director, Joint Requirements Office, Chemical, Biological, Radiological and Nuclear Defense (J-8), Joint Staff ....	104
Klein, Dr. Dale, Assistant to the Secretary of Defense, Nuclear and Chemical and Biological Defense .....	100
Reeves, Brig. Gen. Stephen, USA, Joint Program Executive Officer, Chemical and Biological Defense Program .....	105
Tether, Dr. Anthony, Director, Defense Advanced Research Project Agency ....	103
Younger, Dr. Stephen, Director, Defense Threat Reduction Agency .....	102

## APPENDIX

## PREPARED STATEMENTS:

Goldfein, Brig. Gen. Stephen .....	159
Klein, Dr. Dale .....	137
Meehan, Hon. Martin T. ....	134
Reeves, Brig. Gen. Stephen .....	157
Saxton, Hon. Jim .....	131
Tether, Dr. Anthony .....	144
Younger, Dr. Stephen .....	152

## DOCUMENTS SUBMITTED FOR THE RECORD:

[There were no Documents submitted.]

## QUESTIONS AND ANSWERS SUBMITTED FOR THE RECORD:

Mr. LoBiondo .....	165
--------------------	-----

---

**THURSDAY, MARCH 27, 2003**
**FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT—DEFENSE SCIENCE AND TECHNOLOGY POLICY AND PROGRAMS**

## STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Turner, Hon. Jim, a Representative from Texas .....	171
Saxton, Hon. Jim, a Representative from New Jersey, Chairman, Terrorism, Unconventional Threats and Capabilities Subcommittee .....	169

## WITNESSES

Andrews, Dr. A. Michael II, Deputy Assistant Secretary of the Army for Research and Technology .....	175
Cohen, Rear Adm. Jay, Chief of Naval Research, Department of the Navy .....	178
Engle, James, Deputy Assistant Secretary of the Air Force (Science, Technology and Engineering) .....	180
Sega, Hon. Ronald, Director, Defense Research and Engineering, Department of Defense .....	172
Tether, Dr. Anthony, Director, Defense Advanced Research Project Agency .....	185

## APPENDIX

## PREPARED STATEMENTS:

Andrews, Dr. A. Michael II .....	250
Cohen, Rear Adm. Jay .....	260
Engle, James .....	271
Saxton, Hon. Jim .....	217
Sega, Hon. Ronald .....	219
Tether, Dr. Anthony .....	232

## DOCUMENTS SUBMITTED FOR THE RECORD:

[There were no Documents submitted.]

## QUESTIONS AND ANSWERS SUBMITTED FOR THE RECORD:

Mr. Wilson .....	293
------------------	-----

**TUESDAY, APRIL 1, 2003**

**FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT—  
UNITED STATES SPECIAL OPERATIONS COMMAND BUDGET REQUEST**

## STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Meehan, Hon. Marty, a Representative from Massachusetts, Ranking Member, Terrorism, Unconventional Threats and Capabilities Subcommittee .....	296
Saxton, Hon. Jim, a Representative from New Jersey, Chairman, Terrorism, Unconventional Threats and Capabilities Subcommittee .....	295

## WITNESSES

Billingslea, Marshall, Principal Deputy Assistant Secretary of Defense, Special Operations/Low Intensity Conflict .....	297
Schulte, Harry, Acquisition Executive, United States Special Operation Command .....	317

## APPENDIX

## PREPARED STATEMENTS:

Billingslea, Marshall .....	335
Saxton, Hon. Jim .....	331
Schulte, Harry .....	348

## DOCUMENTS SUBMITTED FOR THE RECORD:

[There were no Documents submitted.]

## QUESTIONS AND ANSWERS SUBMITTED FOR THE RECORD:

[There were no Questions submitted.]

**THURSDAY, APRIL 3, 2003****FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT—DEPARTMENT OF DEFENSE'S INFORMATION TECHNOLOGY PROGRAMS AND POLICIES**

## STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Meehan, Hon. Martin T., a Representative from Massachusetts, Ranking Member, Terrorism, Unconventional Threats and Capabilities Subcommittee .....	373
Saxton, Hon. Jim, a Representative from New Jersey, Chairman, Terrorism, Unconventional Threats and Capabilities Subcommittee .....	371

## WITNESSES

Brown, Rear Adm. Nancy, USN Vice-Director for Command, Control, Communications, and Computer Systems, Joint Staff .....	377
Cuviello, Lt. Gen. Peter, Chief Information Officer/G-6, United States Army ..	394
Gilligan, John, Chief Information Officer, United States Air Force .....	398
Raduege, Lt. Gen. Harry, Jr., U.S. Air Force director, Defense Information Systems Agency .....	379
Stenbit, John, Department of Defense Chief Information Officer .....	373
Thomas, Brig. Gen. John, Department of the Navy, Deputy CIO for USMC .....	400
Wennergren, David, Department of the Navy Chief Information Officer .....	396

## APPENDIX

## PREPARED STATEMENTS:

Brown, Rear Adm. Nancy .....	429
Cuviello, Lt. Gen. Peter .....	472
Gilligan, John .....	484
Raduege, Lt. Gen. Harry, Jr. ....	452
Stenbit, John .....	419
Saxton, Hon. Jim .....	415
Thomas, Brig. Gen. John .....	519
Wennergren, David .....	503

## DOCUMENTS SUBMITTED FOR THE RECORD:

Charts provided by General Raduege .....	537
--	-----

## QUESTIONS AND ANSWERS SUBMITTED FOR THE RECORD:

Mr. Meehan .....	551
------------------	-----



## H. R. 1588

To authorize appropriations for fiscal year 2004 for military activities of the Department of Defense, to prescribe military personnel strengths for fiscal year 2004, and for other purposes.

### IN THE HOUSE OF REPRESENTATIVES

APRIL 3, 2003

MR. HUNTER (for himself and Mr. SKELTON) (both by request) introduced the following bill; which was referred to the Committee on Armed Services

---

### A BILL

To authorize appropriations for fiscal year 2004 for military activities of the Department of Defense, to prescribe military personnel strengths for fiscal year 2004, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

#### SECTION 1. SHORT TITLE.

This Act may be cited as the “National Defense Authorization Act for Fiscal Year 2004”.

\* \* \* \* \*

## TITLE I—PROCUREMENT

### Subtitle A—Authorization of Appropriations

#### SEC. 101. ARMY.

Funds are hereby authorized to be appropriated for fiscal year 2004 for procurement for the Army as follows:

- (1) For aircraft, \$2,128,485,000.
- (2) For missiles, \$1,459,462,000.
- (3) For weapons and tracked combat vehicles, \$1,640,704,000.
- (4) For ammunition, \$1,309,966,000.
- (5) For other procurement, \$4,216,854,000.

#### SEC. 102. NAVY AND MARINE CORPS.

(a) NAVY.—Funds are hereby authorized to be appropriated for fiscal year 2004 for procurement for the Navy as follows:

- (1) For aircraft, \$8,788,148,000.
- (2) For weapons, including missiles and torpedoes, \$1,991,821,000.
- (3) For shipbuilding and conversion, \$11,438,984,000.
- (4) For other procurement, \$4,679,443,000.

(b) MARINE CORPS.—Funds are hereby authorized to be appropriated for fiscal year 2004 for procurement for the Marine Corps in the amount of \$1,070,999,000.

(c) NAVY AND MARINE CORPS AMMUNITION.—Funds are hereby authorized to be appropriated for fiscal year 2004 for procurement of ammunition for the Navy and Marine Corps in the amount of \$922,355,000.

**SEC. 103. AIR FORCE.**

Funds are hereby authorized to be appropriated for fiscal year 2004 for procurement for the Air Force as follows:

- (1) For aircraft, \$12,079,360,000.
- (2) For missiles, \$4,393,039,000.
- (3) For procurement of ammunition, \$1,284,725,000.
- (4) For other procurement, \$11,583,659,000.

**SEC. 104. DEFENSE-WIDE ACTIVITIES.**

Funds are hereby authorized to be appropriated for fiscal year 2004 for defense-wide procurement in the amount of \$3,691,006,000.

**SEC. 105. DEFENSE INSPECTOR GENERAL.**

Funds are hereby authorized to be appropriated for fiscal year 2004 for procurement for the Defense Inspector General in the amount of \$2,100,000.

**SEC. 106. DEFENSE HEALTH PROGRAM.**

Funds are hereby authorized to be appropriated for fiscal year 2004 for the Department of Defense for procurement for carrying out health care programs, projects, and activities of the Department of Defense in the total amount of \$327,826,000.

**SEC. 107. CHEMICAL AGENTS AND MUNITIONS DESTRUCTION.**

Funds are hereby authorized to be appropriated for fiscal year 2004 for chemical agents and munitions destruction in the amount of \$1,650,076,000 for—

- (1) the destruction of lethal chemical weapons in accordance with section 1412 of the Department of Defense Authorization Act, 1986 (50 U.S.C. 1521); and
- (2) the destruction of chemical warfare material of the United States that is not covered by section 1412 of such Act.

## **Subtitle B—Multi-Year Contract Authorizations**

**SEC. 111. MULTIYEAR PROCUREMENT AUTHORITY FOR NAVY PROGRAMS.**

(a) MULTI-YEAR CONTRACT AUTHORITY.—Beginning with the fiscal year 2004 program year, the Secretary of the Navy may, in accordance with section 2306b of title 10, United States Code, enter into multiyear contracts for procurement of the following:

- (1) F/A-18 aircraft.
- (2) E-2C aircraft.
- (3) the Tactical Tomahawk missile.
- (4) the Virginia class submarine.

(b) SHIPBUILDER TEAMING.—Paragraphs (2)(A), (3), and (4) of section 121(b) of the National Defense Authorization Act for Fiscal Year 1998 (Public Law 105-85; 111 Stat. 1648) apply to the procurement of Virginia class submarines under this section.

**SEC. 112. AMENDMENT TO MULTIYEAR PROCUREMENT AUTHORITY FOR C-130J AIRCRAFT FOR THE AIR FORCE.**

Section 131(a) of the Bob Stump National Defense Authorization Act for Fiscal Year 2003 (Public Law 107-314; 116 Stat. 2475) is amended by striking “40 C-130J aircraft” and inserting “42 C-130J aircraft”.

## **TITLE II—RESEARCH, DEVELOPMENT, TEST, AND EVALUATION**

### **Subtitle A—Authorization of Appropriations**

**SEC. 201. AUTHORIZATION OF APPROPRIATIONS.**

Funds are hereby authorized to be appropriated for fiscal year 2004 for the use of the Armed Forces for research, development, test, and evaluation, as follows:

- (1) For the Army, \$9,122,825,000.
- (2) For the Navy, \$14,106,653,000.

(3) For the Air Force, \$20,336,258,000.

(4) For Defense-wide research, development, test, and evaluation, \$18,260,918,000, of which \$286,661,000 is authorized for the Director of Operational Test and Evaluation.

(5) For the Defense Health Program, \$65,796,000.

(6) For the Defense Inspector General, \$300,000.

## **Subtitle B—Ballistic Missile Defense**

### **SEC. 211. RENEWAL OF AUTHORITY TO ASSIST LOCAL COMMUNITIES IMPACTED BY BALLISTIC MISSILE DEFENSE SYSTEM TEST BED.**

Section 235(b)(1) of the National Defense Authorization Act for Fiscal Year 2002 (Public Law 107-107; 115 Stat. 1041) is amended by striking “for fiscal year 2002” and inserting “for fiscal years after fiscal year 2001”.

## **Subtitle C—Other Matters**

### **SEC. 221. RESCIND THE PROHIBITION ON RESEARCH AND DEVELOPMENT OF LOW-YIELD NUCLEAR WEAPONS.**

Section 3136 of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103-160; 107 Stat. 1946) is repealed.

# **TITLE III—OPERATION AND MAINTENANCE**

## **Subtitle A—Authorization of Appropriations**

### **SEC. 301. OPERATION AND MAINTENANCE FUNDING.**

Funds are hereby authorized to be appropriated for fiscal year 2004 for the use of the Armed Forces of the United States and other activities and agencies of the Department of Defense, for expenses, not otherwise provided for, for operation and maintenance, in amounts as follows:

(1) For the Army, \$24,965,342,000.

(2) For the Navy, \$28,287,690,000.

(3) For the Marine Corps, \$3,406,656,000.

(4) For the Air Force, \$27,793,931,000.

(5) For the Defense-wide activities, \$16,570,847,000.

(6) For the Army Reserve, \$1,952,009,000.

(7) For the Naval Reserve, \$1,171,921,000.

(8) For the Marine Corps Reserve, \$173,952,000.

(9) For the Air Force Reserve, \$2,179,188,000.

(10) For the Army National Guard, \$4,211,331,000.

(11) For the Air National Guard, \$4,402,646,000.

(12) For the Defense Inspector General, \$160,049,000.

(13) For the United States Court of Appeals for the Armed Forces, \$10,333,000.

(14) For Environmental Restoration, Army, \$396,018,000.

(15) For Environmental Restoration, Navy, \$256,153,000.

(16) For Environmental Restoration, Air Force, \$384,307,000.

(17) For Environmental Restoration, Defense-wide, \$24,081,000.

(18) For Environmental Restoration, Formerly Used Defense Sites, \$212,619,000.

(19) For Overseas Humanitarian, Disaster, and Civic Aid programs, \$59,000,000.

(20) For Drug Interdiction and Counter-drug Activities, Defense-wide, \$817,371,000.

(21) For the Defense Health Program, \$14,876,887,000.

(22) For Cooperative Threat Reduction programs, \$450,800,000.

(23) For Overseas Contingency Operations Transfer Fund, \$50,000,000.

### **SEC. 302. WORKING CAPITAL FUNDS.**

Funds are hereby authorized to be appropriated for fiscal year 2004 for the use of the Armed Forces of the United States and other activities and agencies of the Department of Defense for providing capital for working capital and revolving funds in amounts as follows:

(1) For the Defense Working Capital Funds, \$1,721,507,000.



(2) For the National Defense Sealift Fund, \$1,062,762,000.

**SEC. 303. ARMED FORCES RETIREMENT HOME.**

There is hereby authorized to be appropriated for fiscal year 2004 from the Armed Forces Retirement Home Trust Fund the sum of \$65,279,000 for the operation of the Armed Forces Retirement Home, including the United States Soldiers' and Airmen's Home and the Naval Home.

## **Subtitle B—Environmental Provisions**

**SEC. 311. CLARIFY DEFINITIONS OF SALVAGE FACILITIES AND SALVAGE SERVICES TO INCLUDE ENVIRONMENTAL RESPONSES AND RELATED EQUIPMENT.**

(a) **SALVAGE FACILITIES.**—Section 7361(a) of title 10, United States Code, is amended by adding at the end the following new sentence: "Salvage facilities include, but are not limited to, equipment and gear utilized to prevent, abate or minimize damage to the environment."

(b) **SETTLEMENT OF CLAIMS FOR SALVAGE SERVICES.**—Section 7363 of such title is amended by adding at the end the following new sentence: "Claims for such salvage services include, but are not limited to, those for enhanced or special compensation for services that prevent, abate or minimize damage to the environment."

**SEC. 312. AUTHORIZATION FOR FEDERAL PARTICIPATION IN WETLAND MITIGATION BANKS.**

(a) **IN GENERAL.**—Chapter 159 of title 10, United States Code, is amended by adding at the end the following new section:

**"§ 2697. Authorization for Federal participation in wetland mitigation banks**

"The Secretary of a military department engaged in any activity resulting, or which may result, in the destruction of or impacts to wetlands is authorized to make payments to wetland mitigation banking programs and consolidated user sites ('in-lieu-fee' programs) that have been approved in accordance with the Federal Guidance for the Establishment, Use, and Operation of Mitigation Banks or the Federal Guidance on the Use of In-Lieu-Fee Arrangements for Compensatory Mitigation Under Section 404 of the Clean Water Act and Section 10 of the Rivers and Harbors Act as an alternative to creating a wetland for mitigation on Federal property for construction projects. These payments may be included as eligible project costs for military construction."

(b) **CLERICAL AMENDMENT.**—The table of sections at the beginning of such chapter is amended by adding at the end the following new item:

"2697. Authorization for Federal participation in wetland mitigation banks."

**SEC. 313. PROVISION TO EXEMPT RESTORATION ADVISORY BOARDS FROM THE FEDERAL ADVISORY COMMITTEE ACT.**

Section 2705 (d)(2) of chapter 160 of title 10, United States Code, is amended by adding at the end the following new subparagraph:

"(C) The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to any restoration advisory board established by the Secretary pursuant to this subsection."

**SEC. 314. REPEAL OF MILITARY EQUIPMENT AND INFRASTRUCTURE: PREVENTION AND MITIGATION OF CORROSION.**

(a) **IN GENERAL.**—Section 2228 of title 10, United States Code, is repealed.

(b) **CLERICAL AMENDMENT.**—The table of sections for chapter 131 of this title is amended by striking the item relating to section 2228.

## **Subtitle C—Workplace and Depot Issues**

**SEC. 321. REPEAL OF TIME LIMITATION ON EXCLUSION OF EXPENDITURES ON CONTRACTING FOR DEPOT-LEVEL MAINTENANCE.**

Section 2474(f)(2) of title 10, United States Code, is amended by striking "for fiscal years 2002 through 2005".

**SEC. 322. EXCEPTION TO COMPETITION REQUIREMENT FOR DEPOT-LEVEL MAINTENANCE AND REPAIR.**

Section 2469 of title 10, United States Code, is amended by inserting at the end the following new subsection (d):

"(d) EXCEPTIONS.—This section shall not apply with respect to depot-level maintenance and repair workload that is the subject of a public-private partnership entered into pursuant to section 2474(b) of this title provided—

"(1) competition is sought to select the source that will partner with the depot to perform the workload;

"(2) the payment requests made by the partnership for work performed reflect the full cost to the Government of resources used by the depot for providing services, which shall include costs of resources used, but not paid for, by the depot;

"(3) the portion of the payment received by the partnership that is necessary to cover the full cost of performance by the depot, as required by paragraph (2), is transferred to the General fund in the Treasury to the extent the payment is reimbursing the depot for federal resources the depot has used, but not paid for, in performing its work;

"(4) in accordance with applicable contracting procedures, the customer agency is not charged for any effort undertaken by the partnership to correct performance deficiencies; and

"(5) the depot does not charge its partner contractor for any effort the depot undertakes to correct performance deficiencies under the contract."

**SEC. 323. EXCLUDE WORKLOADS FOR SPECIAL ACCESS PROGRAMS FROM LIMITATIONS ON THE PERFORMANCE OF DEPOT-LEVEL MAINTENANCE OF MATERIEL.**

Section 2466(d) of title 10, United States Code, is amended to read as follows:

"(d) EXCEPTIONS.—Subsection (a) shall not apply with respect to—

"(1) the Sacramento Army Depot, Sacramento, California; and

"(2) workloads for special access programs."

**SEC. 324. ESTABLISHING MINIMUM LEVEL OF PERFORMANCE OF DEPOT-LEVEL MAINTENANCE OF MATERIEL BY FEDERAL GOVERNMENT PERSONNEL OR AT A GOVERNMENT-OWNED FACILITY.**

(a) ESTABLISHING MINIMUM LEVEL.—Section 2466(a) of title 10, United States Code, is amended to read as follows:

"(a) ALLOCATION OF WORKLOAD PERCENTAGE.—At least 50 percent of the funds made available in a fiscal year to a military department or a Defense Agency for depot-level maintenance and repair workload shall be used for the performance of such workload for the military department or the Defense Agency by Federal Government personnel or at a Government-owned facility."

(b) CONFORMING AMENDMENT.—Section 2474(f)(1) of such title is amended by striking "percentage limitation" and inserting "allocation of workload percentage".

**SEC. 325. CENTERS OF INDUSTRIAL AND TECHNICAL EXCELLENCE: EXTENSION OF PARTNERSHIP EXEMPTION.**

Section 2474(f)(1) of title 10, United States Code, is amended by striking "at" and inserting "for".

\* \* \* \* \*





**FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT—FORCE PROTECTION POLICY: THE ROLE OF THE DEPARTMENT OF DEFENSE AND THE NATIONAL GUARD IN HOMELAND SECURITY**

---

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ARMED SERVICES,  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES  
SUBCOMMITTEE,

*Washington, DC, Thursday, March 13, 2003.*

The panel met, pursuant to call, at 2:00 p.m. in room 2212, Rayburn House Office Building, Hon. Jim Saxton (chairman of the subcommittee) presiding.

**OPENING STATEMENT OF HON. JIM SAXTON, A REPRESENTATIVE FROM NEW JERSEY, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. SAXTON. The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this afternoon for the first time in formal session. Although we have had several informal meetings and briefings, today marks the first public hearing of this important new body, which I am honored to lead in conjunction with our distinguished ranking member, Marty Meehan of Massachusetts. As I said in private but now want to put on the record, I want to sincerely thank all members who have volunteered to serve on this subcommittee and look forward to working with you as closely as we can together as we help the Department of Defense (DOD) and military services to fight the scourge of terrorism. I have proposed and my colleagues support an active agenda, and an active agenda it will be as there is much to be done. Despite the ever growing nature of the terrorist threat at home and abroad which culminated in the tragic events of September 11, the Armed Services Committee has never before established a standing committee to address the many issues involved. It is our duty to be diligent, and very diligent we will be. While recognizing that we cannot accomplish everything immediately despite our collective sense of urgency, our first hearing is a fitting start. We not only begin with the general view of the Department of Defense, which is logical, but there is an interesting contrast of the old and new and the distinguished positions that our witnesses hold.

Let me explain. Our first witness, the Honorable Paul McHale, while a gentleman of extraordinary abilities, experience and common sense, occupies a brand new senior policy making office in the Department of Defense. He is Assistant Secretary of Defense for Homeland Defense and is testifying today for the first time in that capacity. As part of his responsibilities, he will help to oversee the

work of the Department's newest combat command, Northern Command, whose Commander testified before the full committee earlier today. Both Secretary McHale and General Eberhardt in turn are under the nurturing and watchful eye of this body, the newest standing committee concerned about force protection and homeland defense. That is our new part of the equation that I referred to earlier.

Now to the old at least in lineage. I find great comfort in the fact that an enduring institution of this great country, indeed the institution that fought for our freedom before we were a Nation, is in the forefront of the effort. I am talking of course about the National Guard, or Militia as it was known in the Revolution. The Guard was there at our Nation's birth and continues to perform critical duties in protection of our homeland. Yes, we have some technical questions about how the missions will be performed and we will address those. But I first wanted to recognize the fundamental and continuing importance of the National Guard to American freedom and ideals.

This is the first of a series of hearings we will conduct before our markup in late April, and it sets the stage for those that follow. Our objective today is to begin to get an understanding of the issues that face the Department of Defense as it commences its coordination efforts with the new Department of Homeland Security in an attempt to learn how we can help process either legislatively or through the budget.

Secretary McHale, I don't think you will find a more open invitation of support during your tenure, and we certainly look forward to renewing our friendship and working with you. I would like at this time to turn to my friend and colleague and partner, Marty Meehan, for any comments he may have.

[The prepared statement of Mr. Saxton can be found in the Appendix on page 47.]

**STATEMENT OF HON. MARTIN T. MEEHAN, A REPRESENTATIVE FROM MASSACHUSETTS, RANKING MEMBER, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. MEEHAN. Thank you very much, Mr. Chairman, and I join you in welcoming our witness today, particularly our former committee colleague, Paul McHale. Secretary McHale, it is great to see you again. You were an outstanding Member of Congress. You have been an outstanding public servant over the course of your career, and I look forward to working with you in this new position.

Mr. Chairman, in your statement you pointed out correctly the challenge before us. The Defense Department and this committee must struggle with the harsh realities ushered in by September 11, 2001. We must remain vigilant in our effort to deter any threat against America both at home and abroad and be prepared to respond to any contingency. It is my hope that the discussion today will assist in this endeavor.

Secretary McHale, you step into a brand new position created only recently by the defense authorization process. You have daunting challenges, yet great opportunities as you shape the duties of your new role. As you embark in this effort, I hope you will

consider a few particular areas of interest. First, as I know you agree, intergovernmental coordination is of utmost concern given the structure and nature of this Nation's public institution. Our Federalist system necessarily brings with it a layered approach to crisis response and consequent management with Federal, State and local officials all representing a key part of the effort to combat terrorism at home, and efforts to operationally coordinate the Department of Defense and the newly created Department of Homeland Security will I am sure prove daunting. Secretary McHale, please let us know how we can assist you in this effort.

Second, the role and mission of the Reserves and the National Guard is a large concern. The Guard and Reserve component is an untapped resource in many ways. Perhaps it holds the answer to several of our present day problems. I look forward to hearing the views of all of our witnesses in this area and working further on the matter in the future. Finally, functional coordination will be important as well.

Both the Department of Homeland Security and the Department of Defense have responsibilities for developing effective response technologies. But at the moment DOD seems better in position for success in this area, particularly in the area of chemical and biological defenses. Secretary McHale, during your tenure as Assistant Secretary of Defense, I hope you can implement a vision and working solution for effective coordination of research and development activities.

Mr. Chairman, I thank you for calling this hearing, and I look forward to working with you on these and other matters.

Mr. SAXTON. Thank you very much, Mr. Meehan. Let me just say at the outset that there are unfortunate—we have reorganized the subcommittee structure on the Armed Services Committee and we now have six subcommittees and we have found that in scheduling that it is virtually impossible not to have conflicts develop between hearings that the subcommittees are holding. The Force Projection Subcommittee is holding a hearing next door and obviously some members are members of both subcommittees, and that is the reason that you see some empty seats here.

We have two panels of witnesses for our proceedings this afternoon, and I would like to welcome our first witness, obviously the Honorable Paul McHale, Assistant Secretary for Defense for Homeland Defense. As I noted in my opening remarks, Paul McHale is not only a former Member of Congress but a distinguished former member of the Armed Services Committee as well. We are pleased that he is serving in this new capacity and we welcome his testimony. And I may also note that he is a Marine and I am very proud to say that my nephew is a brand new Marine, who is currently at the School of Infantry at Lejeune. So, Paul, welcome. We look at you as part of our family. We look forward to your testimony, and I will state, without objection, your prepared statement will be entered into the record.

Mr. Secretary, the floor is yours.

**STATEMENT OF HON. PAUL MCHALE, ASSISTANT SECRETARY  
OF DEFENSE FOR HOMELAND DEFENSE**

Secretary MCHALE. Thank you. Sir, distinguished members of the subcommittee, it is a pleasure and an honor to return to this historic room. It is indeed a privilege to appear as the very first witness of this subcommittee. As noted, Mr. Chairman, I have submitted my formal statement for the record, and what I would like to do with your permission is briefly summarize the content of that statement as previously presented to the subcommittee.

President Bush has said that the world changed on September 11, 2001. We learned that a threat gathers on the other side of the Earth and can strike our own cities and kill our own citizens. It is an important lesson, one we must never forget. Oceans no longer protect America from the dangers of this world. We are protected by daily vigilance at home and we will be protected by resolute and decisive action against threats abroad.

Mr. Chairman, at the outset, we should recognize that America's first line of domestic defense really begins overseas and results from the capabilities of our forward deployed forces. In that sense, Secretary Rumsfeld has correctly noted that the annual homeland defense budget of the Department is in reality \$380 billion. In fact, every dollar that we spend on defense ultimately protects our Nation, whether that is spent on defenses that are located within the Continental United States or reflected in the wartime activities of forward deployed forces on the other side of the globe.

Secretary Rumsfeld recognized in the wake of the barbaric events of September 11 that there was, indeed, a need to create a combatant command with the assigned responsibility to defend the United States of America, our citizens, our territory and, most importantly, our freedoms. The mission of Northern Command reads as follows: The United States Northern Command conducts operations to deter, prevent and defeat threats and aggression aimed at the United States, its Territories and interests within the assigned areas of responsibility; as directed by the President or Secretary of Defense, provides military assistance to civil authorities, including consequence management operations. The Northern Command's (NORTHCOM's) responsibilities essentially fall into two categories, the warfighting defense of the area of responsibility and civil support.

Mr. Chairman, we will fail in our mission if all we do is get better and better at cleaning up a successful enemy attack. Our first responsibility is to defeat that attack as far from our shores as possible. NORTHCOM has that responsibility within its Area of Responsibility (AOR). If we are unsuccessful in the first instance and if an enemy attack is tactically successful, it is the responsibility of Northern Command in cooperation with and in support of civil authorities to provide the necessary military forces in order to guarantee an adequate response and to do so in a timely manner. NORTHCOM's force structure is modest. There are very few forces permanently assigned, although appropriate units have been identified for possible assignment as needed.

The Commander of NORTHCOM is Air force General Eberhardt. It is my understanding he testified before this committee this morning. He is a superb officer and has taken charge with tremen-



dous focus and dedication of what I believe is a tremendously important military command. His headquarters is located at Peterson Air Force base in Colorado Springs in Colorado.

And on October 1, 2002, NORTHCOM achieved initial operational capability. In conjunction with the recognition that we needed to create a new combatant command to defend the United States of America, there is a similar recognition that we needed to create an appropriate office for civilian oversight. Accordingly, in the Defense Authorization Act of 2003, we created—you created by statute the position that I am now honored to fill, Assistant Secretary of Defense for Homeland Defense. We exercise oversight of all homeland defense activities of the Department of Defense. The initial focus but not the only focus is upon NORTHCOM.

As members of this body will be quick to emphasize, there are portions of the United States external to the NORTHCOM AOR. And so we have the responsibility to exercise oversight not only with regard to Northern Command but also with regard to Pacific Command, Strategic Command (STRATCOM), Transportation Command (TRANSCOM), and indeed all of the combatant commands insofar as they interact with homeland defense responsibilities.

I was nominated by the President in January and confirmed approximately 1 month ago. One of the issues that you will explore not only today, I suspect, but into the foreseeable future is the prospective relationship between the Department of Defense and the newly created Department of Homeland Security. We in the Department of Defense believe fairly strongly that close coordination, joint training and exercises must be carried out in order to guarantee that civilian authorities and military forces are properly coordinated into a single effort. And when we provide support to civilian agencies, it is indeed just that. The civilian agency in the United States will under all circumstances take the lead. We will provide support as appropriate. The military chain of command throughout that process will be preserved. There are no assigned forces in the Department of Homeland Security. The military chain of command goes from the President of the United States to the Secretary of Defense to the Combatant Commander who is tasked with the responsibility. But we will support upon order of the President those activities where the capabilities of the Department of Defense may be unique in that they don't exist within the civilian sector or under extraordinary circumstances where civilian authorities may be overwhelmed by the magnitude of the task.

Finally, Mr. Chairman, in my opening remarks let me touch briefly on the role of the National Guard. I have indicated in a number of prior statements that the National Guard must remain a balanced force. The National Guard historically has provided the strategic reserve with regard to overseas combat. I believe that that responsibility will remain. I also believe that consistent with its force structure and end strength, we will see an enhanced homeland defense mission for the National Guard. There are those who would argue that the National Guard should be exclusively dedicated toward overseas warfighting or, in the alternative, exclusively dedicated toward homeland defense missions. In fact, we must achieve both. The lesson that we learned on September 11

was that a determined enemy will attempt to attack the United States, both abroad and at home. The National Guard can play an extremely important role, in fact perhaps a central role in responding to those threats that manifest themselves within the United States.

Mr. Chairman and members, I can assure you that today as always America's men and women in uniform stand ready to defend our Nation against any threat either at home or abroad. Mr. Chairman, that concludes my opening statement, and I would be more than happy to respond to your questions.

[The prepared statement of Secretary McHale can be found in the Appendix on page 52.]

Mr. SAXTON. Thank you very much. Let me turn first to the ranking member, Mr. Meehan, for any questions that he may have at this time.

Mr. MEEHAN. Thank you very much, Mr. Chairman. Mr. Secretary, I visited Natick Labs at our National Protective Center. They had been part of the Federal effort to assist State and local law enforcement entities. What role does the Department of Defense play in transitioning military technology to the civilian first responder world and are there any examples that you could provide to the committee?

Secretary MCHALE. Mr. Chairman, the role is not only one that is based upon appropriate policy, it is a statutory obligation. The National Defense Authorization Act of 2003 required that the Department of Defense appoint an individual who would be responsible within the Department for the transfer of technology when appropriate to civilian agencies. We have not yet done that, but I anticipate that either I or a subordinate in my office will be tasked pursuant to the statute. The area where I think there is an extremely high likelihood that technology developed within the Department of Defense would be both applicable and appropriate for transfer to civilian authorities relates to weapons of mass destruction and remote sensing capabilities. We obviously within the Department seek to develop the very best capabilities we can to detect weapons of mass destruction, whether they be radiological, chemical, biological or even perhaps nuclear. That same kind of detection capability has an appropriate, indeed an essential role in civilian society. And so as we develop those kinds of remote weapons of mass destruction (WMD) sensing capabilities for the military, I certainly anticipate that we will, consistent with appropriate constraints and guidelines, make every effort possible to quickly bring that same capability to the civilian community.

I mentioned just a couple of moments ago, we will intervene at the direction of the President or the Secretary of Defense to provide civil support when we have a unique capability or civilian authorities are overwhelmed. It is our hope that on fewer and fewer occasions will it be determined that we have a unique capability because it is certainly our hope as a department and I believe as a Nation that civilian capabilities will become more robust, that with that technology transfer, capabilities now only found within the Department of Defense will be soon found as well within the civilian community.

Mr. MEEHAN. I think, Mr. Secretary, there is enormous potential. As I visited with the National Protective Center, we have made great strides in terms of the uniform, the equipment that our soldiers wear, and it is so applicable to what firefighters ought to have, the technology they ought to have, the technology to be able to identify a firefighter in a burning building, the technology to be able to measure what our police officers or firefighters' health condition is at any point in time. I think there is enormous potential, and I look forward to working with you to make sure that that transition works effectively for those first responders.

Mr. Secretary, discussions that we have had, you mentioned making the National Guard a more balanced force. As I understand it, that means ensuring that the Guard remains a strategic reserve for the military, while at the same time providing substantial homeland defense capabilities. What will be required to make sure that the Guard becomes a substantial homeland defense force?

Secretary MCHALE. Training, equipment and proper coordination with Northern Command. The National Guard brings enormous flexibility as well as talent to our ability to defend the United States at home. The National Guard is geographically dispersed throughout the Nation. The National Guard brings military discipline and organization to a challenge at hand. The National Guard has flexibility in that it is under the command and control of the Governor as opposed to the Secretary of Defense. And so a Governor can immediately respond to a crisis that might occur within his or her jurisdiction. I believe that we need to look at the kind of support we provide, for instance, to the Civil Support Teams, to make sure that those teams will operate in a contaminated environment, have both the training and the equipment that is required and ultimately we have to coordinate those Guard forces which are in State status or perhaps in what is called Title 32 status; that is, when the command and control is exercised by the Governor but the expense related to that military activity is paid for by the Federal Government; that the Guard's activities when the Guard is operating under the command and control of the Governor have been properly coordinated with the overall concept of operations envisioned by the combatant commander in whose AOR the Guard has been deployed. Those are the kinds of ways that the Guard can provide tremendous utility.

It is likely if we were to have a domestic Weapons of Mass Destruction (WMD) event, the first chem-bio forces to respond would not be Title 10 United States forces. The first forces to respond almost certainly would be the Civil Support Teams (CSTs) under the Governor's command and control.

Mr. MEEHAN. Well, as a follow-up to that, if there was a weapons of mass destruction incident on our soil, Northern Command obviously would play a significant role in the government's response. In your view—and I kind of ask this question for Neil Abercrombie, who is raising this issue in the full committee—in your view, what, if any, would the legal restrictions—what legal restrictions might hamper the Northern Command's ability to operate domestically?

Secretary MCHALE. I am familiar with Congressman Abercrombie's views and if I go afield of your question just let me know.



Mr. MEEHAN. Oftentimes Congressman Abercrombie goes afield when raising these issues.

Secretary MCHALE. When it comes to military activity in the United States in a civil support role, we are not the lead Federal agency. It is very likely that almost in any scenario a department probably under the new Department of Homeland Security, Federal Emergency Management Agency (FEMA), for instance, would take the lead. We would provide the military chain of command and the capabilities, but it is only when a civilian agency is unable to address a challenge at hand that DOD capabilities would be brought into play. And so if we had a domestic WMD event, I think it is quite likely that first responders at the county and municipal level would be the ones to first arrive at the scene. Shortly after that, depending upon the magnitude of the event, National Guardsmen probably in State status would begin to arrive. Once it became apparent that a WMD event had occurred, Civil Support Teams again in State status, federally funded but in State status, would likely arrive to provide the initial response. It would be hours, perhaps even a day later, before the first significant Title 10 forces under United States command would begin to arrive.

And that really gets to your question. Once Title 10 forces would arrive, what kinds of legal constraints are there in terms of the response? If we were talking about a WMD, a weapon of mass destruction, event, there are very few legal constraints that would inhibit—in fact I can't think of any legal constraints that would inhibit the Title 10 response. That would be the type of catastrophic event where there would be an expectation that local, State, Guard and United States Title 10 forces would come together as a team to address the situation at hand. Where there are legal constraints, and I know where Congressman Abercrombie has concern is in the area of law enforcement as it pertains to Title 10 forces as opposed to consequence management activities, which I had been describing up to this point. The 1878 statute, the Posse Comitatus Act, on its face makes it a criminal offense to utilize what we now call Title 10 forces for law enforcement unless there is an express authorization for that activity in the Constitution or by statute. The position that has been taken by the Secretary of Defense is that we and the Department see no need to rewrite the 1878 statute and that in its current form it does not pose an unreasonable restriction on what we would be able to do in the event of a catastrophic event or the requirement that we provide civil support. In fact, the Secretary has taken a very cautious approach to this issue in that we in the Department have no desire or intent to enter into law enforcement activity which ought to be performed constitutionally and statutorily by civilian authorities. And so coming at the issue from a different direction, the position taken by the Secretary of Defense reaches a conclusion similar to Congressman Abercrombie in that the current statute is probably satisfactory.

The only caveat we place to that is this. In the other body, the Senate, there has been some interest in conducting hearings on this subject. And although we are not advocating any change in the statute, we will fully cooperate with this body or the Senate in any review that a member might want to initiate with regard to posse comitatus, but we are not seeking a change in that law.



Mr. SAXTON. Mr. Secretary, during the hearings preceding this hearing and particularly in the full committee, we have been hearing reoccurring themes in briefings and testimony. One of the themes that you articulated as well in your opening statement is that we need to stop the bad guys, if you will, as far from our shores as possible. And I would like to ask if you would expand on your vision of how your office in conjunction with Northern Command might visualize carrying out that part of the mission. And also the other reoccurring theme is that intelligence is critical to achieving our goals. And is there anything that needs to be done at our level or yours to better integrate intelligence with our operational capabilities?

Secretary MCHALE. The answer to that latter question is yes, and that activity is already underway within the Department of Defense. In the same piece of legislation that created the job that I am now privileged to hold, a new position was created for Under Secretary of Defense for Intelligence. That position, which is now held by Secretary Cambone, or soon to be Secretary Cambone. He has been confirmed by the Senate. I am not sure if Mr. Cambone has been sworn in. That position will be the senior position of the Department of Defense with the responsibility to fuse intelligence sources worldwide.

I have already spoken with Mr. Cambone regarding the need to bring a homeland defense perspective to that intelligence fusion. It is one thing to collect raw data. It is something else to review it in terms of its potential impact on homeland defense activities. I am confident that Mr. Cambone in his new position will move dramatically in the direction that I think is implied by your question.

Second, it was for a very specific reason that I read the mission statement of the Northern Command (NORTHCOM) during my opening statement. That statement says, as I noted earlier, that NORTHCOM has the responsibility to deter, prevent and defeat threats and aggression aimed at the United States. In the wake of what happened on September 11, there was an understandable but I think short-term focus on the exclusive portion of the mission that deals with consequence management, and that remains an important responsibility for Northern Command. But we will fail if all we do is get better and better at cleaning up after an attack has been successful. The American people expect more than that from us, from all of us. Northern Command understands the responsibility to develop a strategy that effectively defeats enemy attacks before they come to our shore. So as you look at the component parts of Northern Command, although it is not a formal part of Northern Command, General Eberhardt has a dual command in that he is the Commanding Officer of North American Aerospace Defense Command (NORAD) as well as the Commanding Officer of NORTHCOM. NORAD provides the protection of our air space not only above the United States but above Canada as well. NORTHCOM incorporates that kind of responsibility and supplements it with the additional responsibilities related to maritime defense and land defense. For reasons we have discussed earlier, it is unlikely that NORTHCOM will be assigned significant land forces because the Area of Responsibility (AOR) covers the Con-

tinental United States, where we believe the counterterrorism activity should be led by civilian law enforcement authorities.

With regard to the maritime defense and without going into great detail, I believe there is an urgent need to create within the maritime buffers on either coast of the United States the same kind of comprehensive defense in-depth that has been created over our air space and implemented by NORAD. So my hope would be that with very serious commitment of planning and resources we could establish a maritime defense in-depth that would create upon the oceans the same kind of defensive capability we have already established within the air space of the Continental United States and over Hawaii, Alaska and the Territories of our Nation.

Mr. SAXTON. Thank you. If the efforts to keep the threat at a distance in fact fail and there is a successful tactical attack, do you feel comfortable that the command and control arrangements are in place to enable the appropriate agencies to respond?

Secretary MCHALE. Mr. Chairman, if I ever used the word "comfortable" as it relates to my position, I will probably resign immediately thereafter. I am not comfortable, but I believe that an extremely diligent effort has been made not only with regard to command and control, but also with regard to the operational capabilities. We can always get better, and we will be focused with an urgency to get better every day to a degree that I think will meet with the satisfaction of this committee.

In terms of command and control, we had to explore relationships that had not previously existed. This is a new combatant command. The forces for the most part have not yet been assigned to that command. With regard to land capabilities those forces will not be permanently assigned so we had to establish a command and control structure that enabled a combatant commander to reach across service boundaries and influence the training of equipment and forces that have not yet be assigned to him. He has to influence those forces because although today they belong for the most part to a service, tomorrow in the wake of an event, an attack, those forces could become his.

And then last, we have to coordinate command and control so it is compatible with the lead Federal agencies we are likely to support in the event of a domestic attack. So the coordination is not only within the military, it is external to the Department of Defense across the seam that we intend to close between the Department of Defense and the Department of Homeland Security. But I can tell you today, the command and control capabilities are the best that we can possibly achieve, considerably better than they were a year ago, significantly better than they were 6 weeks ago, but they can always get better.

Mr. SAXTON. In my first question I asked about intelligence and you responded I think very appropriately. There is also a domestic intelligence piece, which I would hold up as an example in asking this question. We task the federal agency, Defense Advanced Research Projects Agency (DARPA), to find a way to help federal agencies communicate better within the structure which currently exists and between themselves. The system that came out was called the Total Information Awareness System (TIA) and it points out a difficulty in making some changes that we ultimately need

to make to enhance our ability to collect and share information. I guess my question is holding TIA as an example, will you be making the recommendations as to how the way we do business not just with collection and sharing of information but, for example, if the FBI needs to have a more robust something, would you be making recommendations, or FEMA needs to do their job in a different way, would you be making recommendations along those lines, or if we need to restructure the way military departments work together, will you be making recommendations along those lines just as some examples?

Secretary MCHALE. The answer is yes. If the improved operational capability relates to the ability of the Department of Defense to conduct a military mission in support of a lead Federal agency, we will join with that lead federal agency in seeking the resources and the guidance from Congress to make sure that the necessary change takes place. This is a partnership. One of the lessons learned, I think, by September 11 was the need for open and cooperative cooperation among governmental entities, not only at the Federal level, but in fact at the State and local level as well, so that within appropriate constraints related to operational security, we all need to talk to each other in greater detail so that when operational capabilities have to be employed, those capabilities can be brought together in a unified effort. And so with regard to, for instance, information sharing, it may well be that the Department of Defense has the unique ability to develop technological capabilities for communication that no one else by definition would have. I think as was proposed with TIA and might be proposed with regard to other programs, the Department would likely develop the technology but then not operationally employ it. Once the technology for communication is developed, if there are policy-based sensitivities, the likely course of action would be for that kind of technology to be transferred to a civilian law enforcement agency subject perhaps to judicial oversight and certainly subject to Congressional oversight so that the use of that technology would then be in conformity with the law. We have technological capabilities, including R&D capabilities, within the Department of Defense that are extraordinarily better than you might find anywhere else. We are dedicated to developing that technology and, when inappropriate for DOD use, openly transferring it to a civilian agency subject to Congressional oversight and operational employment.

Mr. SAXTON. Thank you. I will ask one final question and then turn to Mr. Turner—it is Mr. Wilson's turn. This is an observation and I will make the observation and then ask you to make an observation subject to the topic. It happens to be intelligence once again because I think you will probably agree with me this is one of the most important issues we have to deal with for the following reason. During the Cold War, we developed a robust intelligence collection agency that was developed and geared to meet the threat of the Cold War. That threat involved an enemy that was not hard to see, which was in many ways quite predictable. We knew their tactics. We basically knew what their hardware looked like and in many respects we knew what to expect, and the intelligence was there which gave us the capability to deal with it. Around about 1992 and 1993, as was expressed back at that time by our Vice



President, who was then Secretary of Defense, he said I have got good news and bad news. The good news is the Soviet Union is going to go away, the bad news is the threat isn't. It is just going to change some. Beginning in about 1993, soon after the Vice President made that statement, we collectively took advantage of an opportunity to relax our intelligence capabilities some. Some think too much and I happen to be in that group. At the same time—and the new threat was developing or the threat was changing, so that we no longer—we had relaxed the old capability and in relaxing we were not developing a new capability nor do we even recognize maybe that we needed a different kind of intelligence. Today, as has been pointed out, we need a smaller force to deal with the threat that we normally talk about in this group, terrorism at least, in a much different military capability. And I would make the point that we may need a much different intelligence capability, much different than it was during the Cold War, much different than it was during the 19s. And I happen to believe that that is one of our very basic and most important challenges.

Would you respond and let us know how you see that situation?

Secretary MCHALE. Mr. Chairman, you and I have known each other for quite some time in the context of Congressional representation, but in other parts of past activity I have been an infantryman for almost 30 years. I don't want the enemy to get into my wire. I want to reach out and defeat an enemy threat as far forward of my position as I possibly can. And I will use every weapon available to me to accomplish that mission at the greatest possible distance. With regard to intel, I believe that as we have a defense in-depth established to protect the United States of America, the very first layer of that defense is a worldwide intelligence capability, robust capability, involving both technological means of information collection and human intelligence as well. That has to be a profoundly robust capability capturing every conceivable threat which might ultimately impact upon the United States of America. And then once we gather that data in as powerful a methodology as possible, we need to bring to it, really for the first time in our Nation's history, a homeland defense perspective so we not only have the information, we analyze it in a way that makes clear how that information may be threatening to our fellow citizens, our territory and our freedoms. We cannot wait for the enemy to get into the wire.

And so I believe that the position of Under Secretary of Defense for Intelligence combined with the Terrorist Threat Integration Center that was proposed by the President in his State of the Union Address, we will for the first time recognize that a terrorist threat potentially possessing weapons of mass destruction is out there, that that threat can become imminent and we need to bring to the collection of that intel a homeland defense perspective that was not common if at all in existence during the Cold War.

As a practical matter I begin each day with intelligence briefings, and when those briefings began a common phrase for me was what does this information mean as gathered on the other side of the world in terms of its potential impact on the United States of America? So it is not only better collection, it is better analysis. And I think the new position of Under Secretary of Defense for In-



telligence in cooperation and coordination with the Terrorist Threat Integration Center will dramatically improve that process.

Mr. SAXTON. Thank you, Mr. Secretary. Thank you very much. Mr. Wilson, gentleman from South Carolina.

Mr. WILSON. Thank you very much, Mr. Chairman. And Mr. Secretary, I appreciate you being here today and I had heard of your service with the Marine Corps Reserve and heard about it in the right way from a Marine Corps officer who was bragging about you. So it was a very positive situation and of course I am particularly honored. I represent Parris Island, where we train the chairman's nephew. So that is where he got the excellent training, at Parris Island.

Secretary MCHALE. In the Marine Corps they say we win battles and make Marines, and that is half the equation.

Mr. WILSON. That means a lot for our State to participate in the defense of our country through training. And I particularly appreciate your background as a reservist because you know of the capabilities of the National Guard and Reserves. And this has been an extraordinary day for me in that General Eberhardt was very clear of the central role, as you also indicated, of the National Guard and the recognition that the National Guard is familiar with communities. It knows the geography, it knows the people, there is networking of people. People with civilian backgrounds knowing the communities is just so helpful, particularly in a time of catastrophe. And so I want to thank you all for recognizing that. And I know the Guard is trained, willing and is prepared for that role, and I just want to thank you for what you have done to promote that.

A concern, though, that I do have is really the one of the chairman, and that is intelligence, and probably the questions need to go to Secretary Cambone, but I am concerned about connecting dots. From your perspective do you believe that the intelligence agencies are coordinating enough in trying to address the concerns that people have?

Secretary MCHALE. This really comes back to the kind of comment I made earlier in response to the chairman's question. The cooperation is dramatically better. The lesson—

Mr. SAXTON. If I may just interrupt you for a minute. We are going to have a 15-minute vote and 5-minute vote, and my suggestion is we stay here until we have 5 minutes until the first vote and go and be back shortly.

Secretary MCHALE. I think there is a shared conviction that all of the relevant agencies, those within the Department of Defense, those external to the Department of Defense but within the Federal Government, and those law enforcement agencies at the State and local level need to share information more effectively. What I am sensing is a dramatic change in attitude and culture brought upon us by the enemy attack open September 11. No one—no one I have met has acted in the least way parochially since I have been in this position. There is a strong desire on the part of all concerned to make sure that information essential to a stronger defense is shared by all those who possess it. The hesitation that you heard earlier arose out of the intense commitment in our office that we will get better and better and better every day. And so when we

have a change in attitude that is a significant improvement and a change in technology that allows for the sharing of information more expeditiously, we will then look at the status quo and see how we can make it better.

So I want to communicate to you a sense of satisfaction that the sharing of information, the sharing of intelligence is much better today than it has been historically, but it is an ongoing mission requirement where we can in fact achieve improvement. We are the best in the world at this, even if the Archangel Gabriel came in and sat by my side this is the best information sharing system that human beings can at the present time create, we would try to do better.

Mr. WILSON. I am delighted to hear that because it concerns me so much that we have great intelligence, but trying to put it together and getting it to the right people is going to be so crucial. In line with technology, it is my understanding that two information technology efforts are being fueled in DOD that could be better suited for the Department of Homeland Security. The Homeland Security Command and Control System sponsored by the Northern Command and Protect America, abutting data sharing system, should DOD be developing these systems or DHS?

Secretary MCHALE. That is Project Protect America that you are referring to?

Mr. WILSON. Yes.

Secretary MCHALE. DOD should be developing that system, but the recommendation that I provided is that we should not operationalize it. There are technologies that can only be developed at the present time by the Department of Defense. I think it is reasonable, though, though I hesitate to speak in any way that reflects a judgment regarding the capabilities of the Department of Homeland Security, but my sense is that the Department of Homeland Security probably could not today develop that kind of information sharing technology. And I think you would find almost a consensus that only the Department of Defense or certain high end developers in the private sector might have that kind of capability. But I have also said that if we develop that kind of technology consistent with the testimony I gave to the Senate with regard to TIA, once the technology is developed because of the policy issues that are involved, it probably ought to be migrated for operational purposes out to a civilian law enforcement agency subject to statutory constraint, judicial and Congressional oversight.

So the issue on the first instance is should DOD develop the technology? My answer would be yes. Should the Department of Defense operationalize it? Probably not. Should it be operated by a civilian agency such as the Department of Homeland Security? Yes.

Mr. SAXTON. Mr. McIntyre.

Mr. MCINTYRE. Welcome, Secretary McHale. We are very proud of you and pleased to have served with you on the Armed Services Committee. I know recently you were at North Carolina, Camp Lejeune, and you may also be familiar with the NORTHCOM National Guard program. They currently have an Academy of Counterterrorism that has worked extremely effectively, that already has the facilities, already has the training program and al-

ready has the opportunity to help share that perhaps as a role model we would hope nationally. And I would like to offer to you and I would like to ask you in this need to train over one-and-a-half million law enforcement line officers to find a solution that we could go ahead and start moving to implementation if the NORTHCOM International Guard program that is already established with the curriculum and the capability that could be filled within 90 days would be of assistance to the Department of Homeland Security and if that would be a possible offering that our NORTHCOM International Guard could make to help you.

Secretary MCHALE. My hope is that the folks who are attending the hearing with me from our staff are writing vigorously behind me. I can't see them. That is a hint, guys. I am not familiar with that program, but it certainly seems to me that like some other programs in North Carolina with which I am familiar, it could serve as a model. We would need to review it more carefully. I note very briefly when I was in Onslow County, North Carolina and visited with the emergency management personnel, I became familiar with another example of this kind of coordination that they called the Military Civilian Task Force for Emergency Response, and I frankly felt when I looked at that example of what could be achieved in terms of military civilian coordination, it seemed to me that that precise example might well be a nationwide model. They call it a MCTFFER, Military Civilian Task Force for Emergency Response. And in fact we are now actively looking at the fact of proposing such MCTFFERs at the State level in every jurisdiction. And the model that we look toward was the one I first became familiar with when I visited Onslow County.

Mr. MCINTYRE. Thank you, and I hope that this additional resource, the NORTHCOM National Guard and the Academy of Counterterrorism, is already established and already underway and has the facility to help. We offer that hope that you will gladly follow up.

Secretary MCHALE. This highlights the value and the flexibility of the National Guard. Counterterrorism within the United States is not a military mission, at least in terms of Title 10 forces, meaning the Navy, Army, Air Force, Marines. Counterterrorism in our country is typically led by the FBI and other law enforcement agencies. We within the Department of Defense pursuant to the statute that Mr. Meehan raised earlier, Posse Comitatus Act of 1878, cannot normally become involved in law enforcement activities, but the National Guard, which is not a Title 10 force, when retained in State status may at the direction of a Governor and historically has at the direction of Governors been involved under emergency circumstances in law enforcement activities. So as we look at counterterrorism in law enforcement, that is an area for appropriate National Guard activity subject to State law, and that is precisely where National Guard forces can be used in which Federal Title 10 forces may not lawfully be employed.

Mr. MCINTYRE. Thank you, Mr. Secretary.

Mr. SAXTON. Mr. Secretary, as you know but others may not, we are having two votes. The first one is 15 minutes and there should be 5 or 6 minutes left. So we will go over and get that vote, and we should be back in 15 minutes.

[Recess.]

Mr. SAXTON. Mr. Larsen, would you like to ask your questions at this time, please?

Mr. LARSEN. Thank you, Mr. Chairman. That is the value of rushing back from a vote, or hanging around long enough. It does not matter how far down on the dais you are sitting, if you hang on long enough you get a chance. I appreciate the chance to ask a few questions.

Mr. Secretary, we have talked about weapons of mass destruction and preparing for that. How big do you think the threat of cyberattacks are, and what role do you have in that, and what role does DOD have in preventing cyberattacks and enhancing cybersecurity, for lack of a better term? That is sort of a cliché term.

Secretary MCHALE. There are a few areas that could logically be placed within homeland defense that, because of their jurisdictional responsibility, have been assigned elsewhere.

The cyberdefense of the United States could obviously be included in a list of homeland defense responsibilities, but in fact a policy decision has been made in this area, and a few others, reflecting in most instances the highly technical issues that are involved, to assign instead the responsibility to someone other than the Assistant Secretary of Defense for Homeland Defense the responsibility, or assign the responsibility to a combatant command other than NORTHCOM.

So let me answer the question, I guess, in reverse order. NORTHCOM generally does not have a responsibility to defend the Nation against a cyberattack. To the extent that the military is engaged in that mission, I believe it has been assigned to STRATCOM, the Strategic Command.

It has not yet been determined the degree of oversight that will be exercised by my office, Assistant Secretary of Defense for Homeland Defense, because we have by statute the overall supervisory responsibility for all homeland defense activities of the Department of Defense.

I can tell you that STRATCOM will take the lead in terms of the assigned combatant command, but it has not yet been determined to what degree my office will exercise oversight with regard to STRATCOM's activities.

Mr. LARSEN. Okay.

Secretary MCHALE. The threat, obviously, is real. I should have emphasized that at the beginning of my answer. STRATCOM, I am confident, will make a vigorous effort to address that threat in terms of defensive capabilities.

Mr. LARSEN. Does your answer mean that you are in the running, or that—

Secretary MCHALE. Yes.

Mr. LARSEN. Where else might it go in terms of providing oversight to STRATCOM?

Secretary MCHALE. It is conceivable that the Undersecretary of Defense for Intelligence might have the primary responsibility for that oversight. The kinds of areas—as an example, the coordination and development of missile defense could conceivably have been assigned to the Assistant Secretary of Defense for Homeland Defense



and could conceivably have been assigned to NORTHCOM, but that was not the decision made. Because of the immense complexity, and the established record of activity with regard to missile defense, the decision was made to assign the development and coordination responsibility for missile defense to STRATCOM.

In a few areas where you have an overlap between substantive activity and geographic relationship, the decision was made to assign the responsibility on the basis of the substance of the activity.

I did not phrase that very well, but I think it is quite likely that, among other offices being considered, the Undersecretary of Defense for Intelligence may well have the primary oversight responsibility with regard to cyberdefenses. Clearly, the decision has already been made that STRATCOM, rather than NORTHCOM, will have that responsibility.

Mr. LARSEN. I guess I will go back to a comment you made earlier about total information awareness. You mentioned that operationally, if and when that is developed, the program is developed, operationally it would move to somewhere outside of DOD. Some concerns have been expressed about total information awareness.

How would it be used? Is it appropriately—can it be appropriately used? Do you have any thoughts about walls, safeguards, parameters under which it could be used in the field?

That seems to be one set of questions being asked about it, or certainly one set of questions I am asking about it.

Secretary MCHALE. If I may, I will put it in context. The Total Information Awareness Program has been a matter of some considerable debate going back over a number of months.

If in fact we had credible evidence that terrorists have brought into the United States a weapon of mass destruction, and if we could not at that point locate such a weapon, the kind of data mining capabilities that TIA would provide could prove to be enormously important in locating and defeating such a weapon of mass destruction.

The technology has been under advancement at the Department of Defense. The concern really has been on two levels: Should we have the technology, and my answer to that question is yes, we should; and should the Department of Defense operate it? No. That has not been the intent from the beginning.

Once the technology is developed utilizing the resources of the Department of Defense, the intent has been to transfer that technology out to the civilian community, particularly to civilian law enforcement agencies, for their employment in order to, in this instance, locate that weapon of mass destruction.

The Department of Defense does not intend to operate TIA, in major part because of the sensitivities reflected in the vote on the Wyden amendment, and the desire that this kind of intrusive but perhaps essential capability be operated by civilians, not by military personnel.

Now, to come back to your question, if I were still in Congress, I would probably have some thoughts as to how the legislation should be written to provide restrictions that would guarantee privacy yet allow us to use that technology when appropriate in light of an imminent threat.

There are ways in which we have, judicially and statutorily, limited this kind of activity in order to protect privacy in the past; but as a Department of Defense official, it would be inappropriate for me to begin to pick and choose among the various types of constraints we have traditionally employed in order to protect not only our security but also our privacy.

Mr. LARSEN. Thank you, Mr. Chairman.

Mr. SAXTON. The line of questioning I think was excellent. I have one final question, Mr. Secretary. Let me just ask it generally.

In terms of medical response, we face some issues here that are really quite unique, particularly in terms of biological attack. I have heard discussions—discussions about discussions that are ongoing in DOD about what the appropriate DOD role might be.

Do you see it as a training role? Do you see it as a function, perhaps, of the National Guard? Do you see it as some combination thereof? Would you just give us your thoughts at this point?

Secretary MCHALE. We will bridge the gap between the status quo and where we hope to be in the not too distant future.

In this area of responsibility, at the present time only the Department of Defense has certain capabilities to provide assistance in a highly contaminated environment involving a weapon of mass destruction.

Mr. Chairman, this is precisely the kind of area where the unique capabilities of the Department of Defense are now available to the Nation if the situation warrants such a response. If we have a catastrophic event involving a weapon of mass destruction, the high end WMD response capabilities of the Department of Defense, at the direction of the President or order of the Secretary of Defense, will be made available to the Nation.

Our hope is that, in combination with a short-term operational commitment, we have an immediate training opportunity, so that the capabilities that we have within the Department of Defense—I will give you an example, the Marine Corps' chemical-biological instant response forces, CBIR, or some of the extraordinary capabilities of SB SEACOM within the Army—should in the not too distant future be replicated in civilian society at the State and local level, and perhaps within other Federal civilian agencies, so that what we have today, which is unique, might be shared and made more effective within the civilian community.

If it were to happen now and if it were a high end event, DOD forces would likely be committed, and we do have contingency plans to support civilian authorities under those extraordinary circumstances.

But I would hope 5 years from now the kind of WMD response capability, including biological, chemical, radiological, even nuclear response capabilities, could also be found within civilian society, so that we in the Department would no longer be unique, and we truly would be a backstop for more robust civilian capabilities.

Mr. SAXTON. Would you see current DOD capabilities migrating—when you say civilian, are you talking about first responder communities, or are you talking perhaps about the Guard community?

Secretary MCHALE. I was thinking, frankly, of the civilian community in the sense of first responders. Our first responders today have limited capabilities in terms of a WMD response.

Mr. SAXTON. You bet.

Secretary MCHALE. We would hope to transfer technology so in terms of commitment and training first responders, without imperiling their own lives, would become more effective in reacting to a domestic WMD event.

I would certainly hope that more robust capabilities could be found at the State level, the emergency management agencies at the State level. I would also hope that within the Federal Government some of these capabilities could become more robust within civilian agencies.

Without commenting for the moment on the current capabilities of any of those agencies, I think there is a clear recognition we have to get better.

Last, the Department of Defense ideally would provide those capabilities that were unique or required by an event so overwhelming that even more robust civilian capabilities would be deemed inadequate for an effective response.

Right now we do the job because we can do it, because we have the capability, and because the Nation needs it. The Department of Defense will not stand by when the Nation needs a response. But our hope is that we become the response of last resort, and that we become more effective in a WMD response within our own civilian agencies, State and Federal.

Mr. SAXTON. In the defense community, it is always good to find ways to migrate various functions to other places other than the military, so that the military can do what the military has to do and other people can do some other things.

Secretary MCHALE. Yes, sir. We are warfighters.

Mr. SAXTON. To the extent that migration takes place, it seems to me there would have to be some significant level of training to help those capabilities migrate. That would be a DOD function, as well?

Secretary MCHALE. Yes, sir. I missed a portion of your question in my response. You asked about the Guard. The Guard plays an extremely important role in this area today. The Congress has now mandated by law that there be 55 civil support teams, at least one in every State and Territory.

Those civil support teams have exceptional but limited capabilities. Training is good but not great. We are going to work with the Guard to take the current level of capabilities, which is quite good, and make it even better; and we will work with the Guard to examine the range of missions assigned to the civil support teams.

Right now, the civil support teams essentially assess a contaminated area. They go in with the appropriate personal protection gear and the correct equipment to assess the nature of the contaminant. They determine what kind of contaminant has been released, and they bring with them a communications package that allows integration of their assessment capability into more robust follow-on forces.

The issue is, should they be limited to assessment and communication. That is where they are at right now. That is something

that, along with a lot of other issues, we will be reexamining in the future.

Mr. SAXTON. Thank you.

Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. SAXTON. Mr. Turner is, incidentally—in the last term we had a Panel on Terrorism which had no legislative authority. Mr. Turner was the ranking member, so we have enjoyed an opportunity to get to know each other in this, or a forum very near to this forum, very close. We look forward to your questions.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. McHale, thank you for being here. You were an outstanding Member of the Congress, and I know you are going to do an outstanding job in your position at the Department of Defense.

I wanted to follow up on some of the earlier questions and responses that you gave that related to the ability of the Department to respond based on the Posse Comitatus Act limitations and the various statutes that in some cases the Governors would have authority over the Guard, and those kinds of things.

I wanted to pose a hypothetical for you, to give you the opportunity not only to talk and think through with us that issue regarding who would respond and who had the legal capacity to respond, but also to allow you to share with us your understanding of the various resources, State, local, Federal, that could be brought to bear in the event of a terrorist threat.

The hypothetical that I wanted to give you was one that would go something like this. Let us assume on April 1 the FBI decides, based on intelligence that they had been gathering regarding a terrorist cell in Albany, New York, that they wanted to go ahead and move on that cell and see if they could take that cell out.

In the process of doing so, let us assume they discovered several computers that revealed certain information that was valuable, one of which was the information that on that same date a terrorist attack was planned on Washington, D.C., by driving a tanker tractor-trailer rig from New York down the New Jersey Turnpike.

The information revealed that the contents of that tanker could be conventional explosives. Plans were also there for the use of chemicals, let's say phosgene could have been carried in the tank, and an explosive device attached to the underside and detonated by the driver of the vehicle. Plans were also there to carry a nuclear bomb. So all three were possibilities.

On learning that information, immediately the FBI sent word to local law enforcement to put everybody on notice up and down the New Jersey Turnpike to look for this tanker, and the information revealed that it was likely to be a Diamond Shamrock Transport tanker, and so they gave everybody notice of what the identification would be.

Let us assume that after word went out through the New Jersey State Police and other law enforcement agencies, that someone working at the toll booth at the New Jersey Turnpike spotted such a truck, picked up the phone, made a call, and said, I think I have seen a truck like the one that has been described.

What agencies, State, local, or Federal, would be called on to respond to intercept and disarm that threat, and what legal issues



would be raised regarding who had the authority to be called upon to do it?

Secretary MCHALE. Mr. Turner, as you pose the question, I think there would be few legal issues. The issues for the most part would be operational.

All of the entities that I can think of which could come into play would be free to do so within the parameters of the law. The issue would be who could most effectively intercept the truck as you have described it.

The primary responsibility for the intercept of the truck would probably fall to the FBI. The truck—by virtue of the nature of the threat, and also the fact that State lines were crossed by the terrorists, that would clearly bring the threat within the jurisdiction—the counterterrorism jurisdiction of the FBI.

The FBI does possess certain high-end very capable operational techniques and equipment to conduct such an intercept, and my expectation is that the team assigned that responsibility would be deployed.

Now, with regard to the Department of Defense, we would not normally have a role to play in domestic law enforcement activity even of this nature, with the exception that the Department of Defense does provide certain classified technical assistance regarding some weapons of mass destruction, and those capabilities would be available if civilian authorities were unable to respond.

Last, while the FBI would probably intercept the vehicle and the Department of Defense would provide contingent support, depending upon the nature of the WMD threat, we would certainly notify all of our consequence management commands such that if there were to be an actual WMD event, as opposed to a threat, we would be fully prepared to provide support to civilian authorities during the consequence management following the detonation of any device.

That is really the way it would work out. Law enforcement, even involving counterterrorism, would be a civilian function. Technical capabilities to defeat the threat would be made available if the FBI or the Department of Justice requested such a support.

Last, if the takedown of the vehicle proved to be unsuccessful, we would immediately put on notice our response capabilities so that these very well-trained, very technical capabilities within the Department of Defense would be immediately available at the direction of the President and Secretary of Defense to reinforce civilian consequence management activities.

Mr. TURNER. I was under the impression, and maybe incorrectly informed, that if there was a threat of a nuclear terrorist attack, that the President had greater authorities to utilize military forces than he would in the event that the threat was a conventional explosive.

Secretary MCHALE. Yes, sir, he does. That is highly classified. I would be more than happy to return to the committee on another occasion and discuss that in detail.

Your statement is correct, but to go beyond that I think would raise some significant issues of operational security.

Mr. TURNER. One of the issues that I think the hypothetical raises is the issue of how to apply what I call the A team to such a crisis.

Secretary MCHALE. I am sorry, sir, apply—

Mr. TURNER. What I call the A team; the best, most prepared, best-equipped, and best-trained unit to do the intercept. I have concerns that we may not be to the point yet in our planning that we have made those determinations.

In many cases, the Department of Defense, as you have suggested in your earlier remarks today, does have the superior force by way of technology, by way of personnel and their training. What I am concerned about and would like to have your help in thinking through and resolving is we want to be sure that in the event we have such a threat that we know that we have deployed the A team to do the intercept to try to prevent the incident.

I am not convinced that we don't have the possibility, if not likelihood, of sending the B team to do the intercept and not be able to accomplish the task. Obviously, in DOD, with the technology that you have, special forces capability, I suspect we would be better prepared to intercept such a tanker in Pakistan than we would be in New Jersey. I think that is an issue that we need to try to determine how to ensure that that is not the case.

Secretary MCHALE. Mr. Turner, in an unclassified setting, let me give you an absolute reassurance that the kind of capability you seek to have does exist. It is well-trained, it is routinely exercised, it is a mature operational capability that goes back many years. Some of the very best warriors we have in uniform have trained for a long period of time to go into precisely the kind of situation you have described when there are certain types of WMD threats.

I think if I were to meet with you in private and discuss with you in detail just how well-trained these forces are, and how prepared they are to move very quickly to eliminate such a threat, you would find the answer to be satisfactory.

I would not want to leave the impression in this hearing today, and particularly I would not want our enemies to believe, that we are unprepared to respond. We are fully prepared to respond to that type of event, and we have practiced to do so for many, many years.

Mr. TURNER. I am reassured to hear that. Because of the classified nature of the information, it also raises the concern that in order to utilize it and make it available, that some of that information may have to be shared with local law enforcement in the event the capability needs to be deployed.

Secretary MCHALE. That capability is fully shared with the FBI. The FBI in this kind of situation would have the lead response assignment with regard to counterterrorism, and the FBI routinely trains with and consults with and compares operational capabilities with the military forces that I generally described during an earlier portion of my answer.

Let me assure you that if this required capabilities beyond those embedded in the FBI response, military forces highly trained, very specialized, would be available to assist the FBI. For many, many years the FBI and the Department of Defense have coordinated a response to the kind of scenario that you have presented.

Mr. TURNER. Thank you.

Mr. SAXTON. Thank you. I appreciated the gentleman's question, and I would say two things. The first is that we will be delving into this, and we have already made plans to do so. So in upcoming events that we have already planned we will be looking at these kinds of things.

The second reason is I appreciate your hypothetical, and would have appreciated it even more if you had designated a different route.

Mr. TURNER. I just want to be sure you are listening, Mr. Chairman.

Mr. SAXTON. Mrs. Susan Davis, please.

Ms. DAVIS OF CALIFORNIA. Mr. Chairman, I appreciate the gentleman's response, and thank my colleague for the question.

Within that category, could you talk a little about some of the ambiguities in terms of who would be responsible? I think you tried to answer something earlier, but we had a discussion I guess yesterday in a hearing. There have been so many hearings lately I can't remember which one it was.

I had taken part in the National Defense University, and we did the tabletop exercise. There were a number of concerns, ambiguities, in terms of first responders versus National Guard and other entities, and in trying to work with the local communities.

Are there some areas where you think we do have some serious ambiguities that really need to be addressed? I am just wondering, how are they being resolved now? How do we work through that?

Secretary MCHALE. The answer to your question is yes. I wanted to reassure Mr. Turner that the ambiguity does not exist at the high level of response that would be required in his hypothetical, but the ambiguities certainly exist. That is why we created a Department of Homeland Security. That is why NORTHCOM was created. That is why my office was created.

The real challenge is to make sure that in terms of how an event would actually evolve—I mean, I came into government on a planning commission in my hometown borough. I spent time in the State legislature, and then the Congress, and now here, so I know what it is like at the lowest level of municipal activity.

If we had a terrorist event, it is likely that the first responders within that community would be the ones who, by definition, got there first. You would have local firefighters and EMTs and other local personnel who would respond.

I am not entirely confident—in fact, I am not confident—that we have adequately addressed the safety and operational challenges at that level of response. We have a tremendous first responder system in the United States. If someone is injured in an automobile accident, we know what to do; but if there is a chemical attack, we are working through the appropriate response. We are doing so diligently and quickly, but a great more needs to be done, and particularly at the local level.

You move beyond that and the Governor in the State, as soon as he finds out it is a WMD attack, a terrorist attack, is likely to call out the Guard forces in the area. They will be under State command and control; they will not be part of the Department of Defense at that point.

The Governor is likely to call out simultaneously his Civil Support Team. That team is also under State command and control, though it is paid for by the Federal Government. They are in what is called Title 32 status.

Then, at the next step, if it is a major attack and it is beyond the capabilities of first responders and emergency management personnel, the Guard and the CSTs, then the Governor may well call the President of the United States and indicate that the problem is beyond the capabilities of local authorities, at which point the President may make a decision to commit Title 10 U.S. Military forces.

We have forces that can respond. They are organized and ready to go. I visited many of those forces in recent days. If a Governor made such a call and if the President directed, the Department of Defense in that extraordinary circumstance would be prepared to respond.

To come to your question, you now have local first responders, State emergency management personnel, Guard personnel, civil support teams, and potentially U.S. Military forces co-occupying the same area. What really has to be worked out is the coordination among those response capabilities. We are, in fact, much better today than we were on September 11, 2001; but I do have to tell you that there is considerable work ahead.

Ms. DAVIS OF CALIFORNIA. I appreciate that. I think certainly at the local level people want to make a strong contribution in that regard. There is some concern, perhaps, that we really will not build on what we know in the communities. I just wanted to state that, as well.

I also had a chance to talk to the Navy Reserve recently about something called the Joint Harbor Operations Center, where we utilize a mobile system like a littoral surveillance system.

Is that anything that you are all working with? I would just ask you to please take a look and see what they are doing around that, and to seek your support for that, as well.

Secretary MCHALE. We will do that.

Ms. DAVIS OF CALIFORNIA. One other question. The folks on Coronado Island—I represent San Diego—are concerned about the security of the aircraft carriers there at North Island. I have to assume that we are looking out for their security, but—

Secretary MCHALE. We certainly are.

Ms. DAVIS OF CALIFORNIA. What are we doing differently that perhaps was not done September 10?

Secretary MCHALE. When the threat condition became more severe approximately a month ago, at the time, as you may recall, when the Department of Homeland Security went from yellow to orange, the Department of Defense in terms of force protection condition in the United States went from Alpha, which is the less restrictive category, to the more restrictive category of Bravo, B.

When the Department of Homeland Security, in consultation with the Department of Justice, decided to lower the threat level from orange back to yellow, we did not make a similar decision with regard to force protection conditions. We stayed at Bravo, and although that is subject to ongoing review, I don't anticipate in the



near term that that force protection condition at a higher level will be diminished in any way.

One of the differences between NORTHCOM and the other combatant commands is that ordinarily a combatant commander establishes the force protection condition within his AOR, his area of responsibility. The decision was made that again, because NORTHCOM is a little different and the AOR covers the continental United States, that the force protection of an installation, including the ships in San Diego, would remain with the service that had jurisdiction over those components.

The Navy ultimately is responsible under current law for the protection of those carriers, but the overall condition in the United States has been raised to a higher level, and is not likely in the near term to be lowered.

Also, I would point out we have, without going into detail—we also have air coverage that is provided called the Air Cap that is provided by NORAD over the continental United States, so the Air Cap is significant and the land protection is at a heightened level. Although it is not the highest level of force protection, we believe that at this point in terms of world events it is the appropriate level.

Mr. SAXTON. Mr. Secretary, thank you very much.

Ms. DAVIS OF CALIFORNIA. Thank you, Mr. Chairman.

Mr. SAXTON. Did you have another question, Mrs. Davis?

Ms. DAVIS OF CALIFORNIA. No. I just wanted to thank you.

Mr. SAXTON. In bringing this portion of the hearing to a close, I just would like to thank you and say throughout the afternoon, both here in this room and when we went to vote, people came up to me one after another and said how pleased they were that you are in the position that you are, and just generally expressing the view that we could not be better served.

Thank you for what you are doing. We know you made some sacrifices to do this, and we look forward to working with you and in following your leadership as we move forward with these issues. Thank you very much.

Secretary MCHALE. Thank you, sir.

Mr. SAXTON. We have had two distinguished military officers sitting in the wings, and as Secretary McHale leaves, let me just introduce our second panel this afternoon. This panel will provide an outline of the issues facing our Nation's Guard's participation in homeland defense.

Our witnesses are Major General Raymond F. Rees, the Acting Chief of the National Guard Bureau, and Major General Timothy J. Lowenberg, Adjutant General of the State of Washington and Chair of the Homeland Security Adjutant Generals Association of the United States.

Let me just say, General Lowenberg, that Mr. Larsen will return. He has an obligation until 4 o'clock, and he will be back to be with us in just a few minutes.

At this point, we are ready to hear your testimony, General Rees and General Lowenberg. Please proceed as you see fit.

## STATEMENT OF MAJ. GEN. RAYMOND REES, ACTING CHIEF OF THE NATIONAL GUARD BUREAU

General REES. Yes, sir.

Mr. Chairman, I am General Rees, Acting Chief of the National Guard Bureau. It is a pleasure to be with you and the distinguished members of your committee, and certainly on this auspicious occasion of the first hearing for your committee.

I am pleased to be here with my colleague, General Lowenberg, who has been a very significant leader regarding homeland security among the Adjutants General. We are grateful for this opportunity to be with you and share our perspectives.

I have prepared a written statement that provides detail, but would like to just highlight a few key points.

Mr. SAXTON. That will be great. We will include it in the record in its entirety.

General REES. Thank you.

The Guard, prior to September 11, was providing an unprecedented level of support to overseas military operations of the various combatant commands. Here at home many people talked about what the National Guard could do for homeland security.

In the aftermath of September 11, however, actions spoke louder than words. The Guard has proven itself once again by rapidly, competently, and with great agility performing both overseas and domestic missions, both Federal and State. You are familiar with these successes. They range from airport security to our operations in Afghanistan. They are covered in the written statement, and I would just move on from here to talk about the future.

The National Guard is poised, we believe, to play important roles in homeland defense, including the ground-based missile defense, air sovereignty and information operations, among others.

In addition to these military missions here inside the United States, the National Guard Bureau will also facilitate military support to civil authorities by the Army and Air National Guard. This includes domestic disaster relief operations, counterdrug operations, and incident management assistance, such as would occur after a terrorist use of a weapon of mass destruction.

As specified in Title 10, the National Guard Bureau serves the Departments of the Army and Air Force as their official channel of communications with the States on all matters pertaining to the National Guard. Recently, we have coordinated with the Combatant Commander of U.S. Northern Command, General Eberhardt, to provide Northern Command with the same connectivity to the National Guard as the several States.

Since the National Guard Bureau tracks State as well as Federal call-ups of National Guard, we are in a good position to provide General Eberhardt with some key situational awareness of State-commanded National Guard operations. This should augment his ability to effectively plan for and manage the overall role of his command.

The Guard Bureau's capability as a two-way channel of communication to the National Guard of the several States is a valuable tool in the homeland defense and homeland security environment. We are pursuing some discussions and initiatives inside the De-

partment of Defense to better exploit that capability for all segments of the Department of Defense.

The protection of our homeland against terrorism is expected to be a protracted endeavor much like the Cold War. To that end, many policy experts, reports, and studies have advocated an expanded role for the Guard in homeland security. Some have suggested that the Guard should be reoriented, reequipped, and retrained predominantly for the homeland security mission.

The reality, however, as Mr. McHale spoke to earlier, is that the Guard is an integral part of the Army and Air Force total force mission capability vital to the survival of the Nation.

In the past, the resources, personnel, equipment and training provided for the wartime mission were sufficient to allow the Guard to also support local and State civilian authorities in responding to disasters or other threats. Times have changed. The threat posed by well-financed, sophisticated, and determined international terrorist groups has raised the bar as to what the National Guard must be able to do.

While the National Guard will continue to maintain a high state of readiness for overseas military operations, it must also better prepare itself to respond to threats here inside the United States. Both at the Bureau and in the States, the Guard is working hard to find ways to meet the increased demands of the homeland security mission while still maintaining its full capability to execute its total force requirements.

The Bureau is working with the States as they identify what homeland security capabilities they need. We plan to consolidate and validate the stated requirements, and then work to help find solutions.

We believe the road ahead also includes a transformation of our current National Guard counterdrug efforts into an integrated counternarcotics/homeland defense counterterrorism program. These mission areas employ many of the same tactics, techniques, and procedures, as well as equipment, training, and skills.

Therefore, a great deal of cross-skill transfer could begin immediately once a change is put in place. Such a transition between and across mission sets will allow National Guard troops to take their places on the front lines of the war against terrorism.

In the brief time we have here today, I have summarized a few of the ideas we are currently working on. I have put more into the written statement, and I would mention to you there are a couple of other educational opportunities that your committee may want to take advantage of.

First, at the Pentagon on March 26 there will be a Civil Support Team there all day long demonstrating their capabilities, and we can set up appointments for your members if they care to see that.

I have also brought with us a white paper on a concept of how the Guard could be used in homeland security, and a short historical document of how the New York National Guard responded to the events of September 11.

In closing, the Guard has helped the Army and Air Force to fight America's wars overseas. The Guard has helped State and local authorities fight floods, forest fires, and riots. The Guard has helped fight the fear and uncertainty surrounding weapons of mass de-

struction with its Civil Support Team. The Guard has helped in the war on drugs with its tie-in with law enforcement.

These successes would have been impossible without the visionary leadership and support we have gotten from the United States Congress over the years. We have every confidence that the same level of Congressional leadership and support will ensure that the Guard achieves its full potential in helping to fight the scourge of terrorism, as well.

Thank you for this opportunity, and I look forward to taking your questions.

[The prepared statement of General Rees can be found in the Appendix on page 63.]

Mr. SAXTON. Thank you very much.

General Lowenberg.

**STATEMENT OF MAJ. GEN. TIMOTHY LOWENBERG, THE ADJUTANT GENERAL, DIRECTOR, WASHINGTON MILITARY DEPARTMENT, AND CHAIR OF THE HOMELAND SECURITY ADJUTANTS GENERAL ASSOCIATION OF THE UNITED STATES**

General LOWENBERG. Mr. Chairman and distinguished members of the committee, thank you on behalf of the Adjutants General of the United States for this opportunity to speak about the role of U.S. Military forces in homeland security and ground truth as we see it from the front lines, from our forward-deployed positions in all of the States, Territories, and the District of Columbia.

The Adjutants General Association of the United States affirms and supports everything General Rees has related to you in his opening statement and in the remarks he has submitted and that this committee has accepted for the record.

The Adjutants General and the National Guard, Army and Air Force, we command are already major players in the States' response plans, and are full partners with emergency management, law enforcement, fire, health, and other civilian emergency responders. We truly are the forward-deployed military forces in America's home theater of operation.

Many of us, and in fact a majority of the Nation's Adjutants General, are dual-hatted as our States senior emergency management official. For example, I not only command our military forces, I also directly oversee all statewide emergency management and emergency-enhanced 911 communications programs.

Second, I coordinate the activities of our State Emergency Management Council and our State Committee on Terrorism in the ongoing work of the 35 Federal, State, and local agencies and private sector organizations such as hospital associations, nongovernmental volunteer organizations, and the like, which work collaboratively to make our State safer from the threats of domestic and international terrorism.

I am a member of the FBI's Joint Terrorism Task Force and the U.S. Attorney's Antiterrorism Task Force.

In my third and distinct role as the State's designated Homeland Security Director, I am responsible for our State's interaction with the White House Office of Homeland Security, newly informed Department of Homeland Security, and other Federal agencies such as the Department of Justice and the FBI.



I also chair the weekly meetings and oversee the daily liaison among the Governors, Chief of Staff, and senior policy advisers and the domestic security members of the Governor's cabinet and our independently elected State Attorney General.

I point out these complex civil-military roles and responsibilities not because they are unique to me or to the State of Washington; in fact, they are not. They are typical of most Adjutants General in most States. I point them out because they illustrate the National Guard's critical role in State response plans and State emergency preparedness strategies; and second, because they reflect the daily roles, responsibilities, and relationships with civil authorities that simply do not exist anywhere else in the American Armed Forces.

These key relationships should not be cast aside in our response to a national security event; they should be the very foundation upon which our Department of Defense fashions its contributions to the incident response.

With the new and expanding range of chemical, biological, nuclear, and radiological threats, response time is critical. With field operations in more than 3,300 communities nationwide, we are the military forces that can react in time to make a difference, from the very earliest stages of an emergency response. We are able to respond quickly and efficiently and with a minimum of overhead and administrative costs because of a standing joint State area command structure which serves as the Adjutant General's mobilization headquarters for all National Guard troop deployments.

When used properly, as they were for deploying thousands of Guardsmen to more than 440 airports following the attacks of September 11, these State headquarters elements are a cost-efficient force multiplier for the Department of Defense.

When not used, as was the case when the Army decided to federalize the National Guard for border security missions in mid-2002, the results are unnecessary costs, extraordinary time delays, operational inefficiencies, and, in many instances, degradation of our combat readiness.

Our State area headquarters are capable of playing a larger role in responding to domestic security events.

As a member of the General Officer Work Group at Northern Command, I, along with other Adjutants General, have been exploring operational courses of action with NORTHCOM that would take better advantage of this National Guard resource.

Mr. Chairman, members of the Committee, let me on a personal note just add my vote of confidence, along with that previously expressed by Secretary McHale, for General Ed Eberhardt, the first Northern Command Commander, an extraordinary individual and truly the best American I know to fill this critical role, and a role that I might note has not been filled since George Washington was a Combatant Commander for the Continental United States. He demonstrates superb leadership, and is an officer who truly understands the nuances and complexities and the various status of the National Guard.

The leaders of the National Guard are ready and eager to contribute in an even more meaningful way to our homeland security, but as part of a dual mission set that includes our continued com-

bat, combat support and combat service support for outside the Continental United States (OCONUS) military operations.

Homeland security is an important mission, but it would be a grave mistake to try to make it the sole or primary mission of the National Guard. I would note again that we speak with one voice with Secretary McHale in urging that we be dual-missioned and dual-resourced to serve the entire spectrum of the needs of the American military forces, and for both homeland defense and homeland security.

Although there may be a need for selected units, such as our Civil Support Teams, to be specially missioned or resourced primarily for homeland security purposes, homeland security can be most effectively and efficiently accomplished as a dual mission that compliments, enhances, and draws its essential strength from the National Guard's continued combat force structure, combat training, and overseas deployment experience.

I mentioned our Civil Support Team, so let me pause to emphasize that we believe strongly that every State and territory should have a Civil Support Team. Only 30 States have a team at the present time, with one other State, Kansas, anticipating certification of a team by the end of this month. The lives of emergency responders and citizens in the 23 remaining States and territories are no less important.

Our association, along with the National Guard Association of the United States, the National Emergency Management Association, the International Association of Emergency Managers, Council of State Governments, and the National Governors' Association urge Congress to fund the 55 teams authorized but not funded by the 107th Congress, thereby providing a team for every State and Territory.

The Guard is clearly capable of doing more and should do more, but much of what we know needs to be done, and much of what the reports of the Hart-Rudman Commission and Gilmore Commission and other thoughtful advisory groups have advocated be done by the Guard can only be accomplished by having the Secretary of Defense recognize these domestic missions as being within the responsibility of the Department of Defense, and by Congress authorizing and appropriating funds to carry out federally-approved homeland security missions.

I would note that Senator Kit Bond of Missouri and Senator Feinstein and others have introduced legislation, Senate bill 215, that is now before the Senate Committee on Armed Services that would authorize the National Guard to execute missions in a Governor's homeland security plan that would be approved by the Secretary of Defense. The bill is patterned after the successful National Guard Counterdrug Act.

We are currently authorized and funded, as many of the committee members well know, for a modest amount of additional training for quelling civil disturbances under the Garden Plot Operation; but this bill would enable us to do much more, from counterterrorism contingency planning and exercises with civilian authorities to protecting critical infrastructure and key assets.

The Adjutants General Association of the United States and the National Guard Association of the United States urge support of this legislation and swift passage.

As I have explained in greater detail in my prepared remarks, the National Guards of the several States are able to respond so efficiently to multistate and regional disasters because of the coordination role or the financial institutions role, if you will, of the National Guard Bureau. By statute, the National Guard Bureau is the channel of communication between the several States and the Secretaries and Chiefs of Staff of the Army and the Air Force.

With the reorganization of the Department of Defense, including the creation of Northern Command, it is important that the Chief of the National Guard Bureau be authorized by statute, rule, and regulation to serve as our channel of communications between the States and the new Military Support to Civil Authority Executive Agent for DOD, Mr. Secretary McHale, and the new Action Agent for DOD, the Joint Staff Directorate of Military Support (DOMS).

I have pointed out the statutory and regulatory changes in my written statement.

Finally, the Guard is unique in the number of legal statuses in which it can be engaged, from State active duty at State expense for natural disasters and other State emergencies not involving Federal interests, to Title 32 duty under State control but with Federal oversight at Federal expense and for Federal purposes, such as our counterdrug missions, our Civil Support Team deployments, and airport security and other such missions; and finally in Title 10 status under Federal control and at Federal expense for Federal purposes, such as our role in 89 countries last year as part of America's globally deployed combat forces.

For the many operational and cost efficiency reasons that I have articulated in my formal remarks, and the attachments to those remarks, the Adjutants General of the United States and the Nation's Governors believe strongly that, with rare exception, when National Guard forces are used for a Federal purpose within the United States we should be in Title 32 status under continuing State control, albeit with Federal oversight and at Federal expense, because of the Federal purpose for the domestic deployment.

I have given the committee a copy of the National Governors' Association resolution on use of the National Guard, which was adopted 3 weeks ago at the Governors' winter meeting in Washington, D.C.

As previously indicated, Mr. Chairman and members of the committee, I have expanded on these and other key issues in my written statement, which I would ask be incorporated in the record.

I look forward, along with General Rees, to responding to your questions. Thank you very much for what you do day in and day out to make America safe and to protect us from the scourge of international terrorism.

[The prepared statement of General Lowenberg can be found in the Appendix on page 72.]

Mr. SAXTON. Thank you very much, Mr. Lowenberg. Your statement will be included in full in the record.

We have been talking about the changed threat and changed functions of various units of the military. It seems to me that one

of the most dramatic changes we have seen, requirements that we have seen, affects the National Guard.

My friends and neighbors—incidentally, I have two little statues in my office. One of them is a little soldier, a soldier with an M-1 rifle kind of charging forward. We call him the ultimate weapon. Right next to him there is a statue of a Guardsman militiaman, and we call him the ultimate patriot. So we understand what you do and the people that work with you and for you, and we appreciate that very much.

But the fact is, as I was saying a minute ago, the requirement for the Guard has changed very dramatically in the last several years. We used to tell our friends and neighbors, come on, sign up. Give us two days a month for training and a couple of weeks in the summertime, and here is your benefit package, and there is a retirement at the end of the road. People signed up for that duty, knowing that they might be mobilized and deployed for a short period of time once or twice in their career. It is not that way anymore, as you know better than I.

I guess I then come to the question that has been raised in my mind and in other's minds here by statements that the Secretary of Defense has made about changing in some ways the role of the Reserves generally.

How do you see those potential changes affecting the Guard?

General REES. Mr. Chairman, we certainly have been attuned to some of those statements, and there has been a lot of discussion.

Certainly there is concern, but as we develop the conversation, we have had the opportunity to actually hear from the Secretary in conversation with the Adjutants General here about two weeks ago where he very strongly stated that he fully supported and sees the National Guard and Reserve as a key element of the total force, and on into the future.

So there are needs for transformation to meet the realities of the 21st century, but it is not to the detriment of the Guard and Reserve the way my interpretation of his remarks are.

General LOWENBERG. I would certainly concur with that assessment, particularly with our meeting with Secretary of Defense Rumsfeld a few weeks ago in Washington, D.C..

We all recognize that we spend about 3 percent of our Nation's gross domestic product on our collective defense, so to seriously be considering fundamentally reshaping the National Guard so we play a lesser role in our combat, combat support, and combat service support functions would require a truly radical change in the apportionment of resources by the Federal Government for our collective defense.

I think the Adjutants General are confident that that what Secretary of Defense Rumsfeld is contemplating is a balanced adjustment of roles and missions that don't really fundamentally detract from the dual missioning that we spoke to earlier in our opening statement.

Mr. SAXTON. Thank you. The most likely changes that I have been able to identify in various conversations with various people have to do with the capabilities that are currently in the Guard and Reserve that are needed on a very frequent, sometimes long-term basis to supplement the active force.



Perhaps there has been some thought given to taking some of the missions of the active force and making some trades with various functions that are in the active force and in the Reserves.

Is that the kind of thing that you see being talked about?

General REES. Mr. Chairman, I think that is exactly what is being looked at to find out what is the right balance. There is a very significant study going on right now in the Joint Staff in regard to that.

General LOWENBERG. If I could comment, Mr. Chairman, some of those missions are within my mission set in my State. We provide part of the air bridge through air-to-air refueling for virtually any deployment of forces anywhere in the world for the U.S. Military.

So in part the answer to your question depends upon how we present forces and how we utilize the Reserve component. If we utilize the Reserve components in kind of a cookie cutter approach that says you can only do your contribution by 179-day commitment and continuous employment as opposed to rotating forces, then you get one answer. If we think in a transformational way about how we present forces and use the Reserve components, we come to a different answer.

I would also note that there is a lot of discussion, for example, about too much civil affairs capability being in the Reserve components. That is a mission area that I oversaw for the Air Force for nearly 5 years throughout the world, to include operations with the U.N. peacekeeping office and operations in Bosnia to enforce the Dayton Peace Accord.

The fact is that the true expertise for reconstituting functioning civil society lies largely in the private sector and lies largely in the Reserve components. So we greatly diminish our ability to provide for America's needs abroad and to represent America's interests if we don't take maximum advantage of what is truly unique in the Reserve components.

Mr. SAXTON. Thank you.

Unless you have something further to add on this subject, I will move on to another question. Thank you.

Secretary McHale talked about the important role of the Guard in meeting various contingencies because of the capabilities under Title 32, which leaves the command of the State Guard in the hands, essentially, of the Governor. Correct?

General REES. That is correct.

Mr. SAXTON. I guess my question is this: Inasmuch as we face a situation like none that we have faced in the past vis-a-vis an attack on our civilian community by foreign entities, and inasmuch as the military function, if you will, of the Guard will be carried out to provide for national security, it is an unusual situation, and I don't say this in a disparaging way about any Governor or any Governor's advisers, but the fact of the matter is that there is a level of training that seems to me to be necessary in order to make or ratify decisions that have to do with the activities and missions of Guard units around the country.

Are there changes that are necessary in the command and control structure so that we make sure that these—that the input is there for the appropriate decisions to be made by people who are

going to make those decisions who are not necessarily—who are almost always untrained in these areas?

General REES. Mr. Chairman, I think that is a very good question. In some regards this relates back to what General Lowenberg just talked about, the way of presenting the forces and what is really required.

If we are talking about force application, as opposed to a civil support response of a humanitarian kind of event, then that clearly ups the ante as far as the training, knowing the rules of engagement, using the weapons properly, et cetera.

I will give an example from your own State. Your New Jersey Air National Guard, has a very good, very fine air defense organization, F-16 organization, that has been flying combat air patrols over the United States.

Mr. SAXTON. We are proud of them. We make sure they are nowhere near the Turnpike.

General REES. There has been a structure put in place through the Air Force' auspices, the North American Air Defense, First Air Force, their operational readiness inspection capabilities, to ensure that these individuals who are predominantly in Title 32 status most of the time—that when they are required to actually go into a force application mode, they transfer immediately through what we call hip pocket orders into Title 10 status and immediately report up the chain of command to First Air Force North American Air Defense Command, and perform the mission and perform it very well. So that is at one extreme.

If in fact there were cases and requirements that the Federal Government saw that we needed to do the same thing and have our National Guardsmen be able to transition from Title 32 to Title 10 and meet that kind of rigorous standard, we could move out and get that accomplished.

On the other hand, we find that those lower end requirements that have to do with the support of law enforcement, that have to do with the support of State and local entities out there—we have a lot more flexibility under State law, and without limitations such as posse comitatus for the National Guard to participate in those events. If again there is a requirement for a higher standard, then certainly the National Guard Bureau, in conjunction with the Northern Command Commander, could establish those standards.

In fact, I would say that would be one of the greatest benefits the Northern Command Commander could have is using the Adjutants General and the National Guard Bureau to establish better standards all across the country.

General LOWENBERG. I might add that the Militia Clause of the U.S. Constitution provides for the military forces of the several States to serve in the service of the United States, that is the term of art, "in the service of the United States," to enforce the laws of the Union to repel invasions and to suppress insurrections.

It sounds an awful lot like a description of homeland security. When we talk about military forces of the National Guard being used in Title 32 status, we are not talking about ad hoc State control, because the Federal Government has to be willing to receive those services, and the Federal Government has to give the green

light that says, yes, this proposed mission is in the service of and in the interest of the Federal Government.

Therefore, just like we did on airport security with no notice at 440 airports throughout the United States, we executed that mission according to the rules of engagement, the rules of force, and the other directions of the lead Federal agency.

General LOWENBERG. The advantages of utilizing the National Guard and Title 32 are really operational. During that 6-month period in which we safeguarded the Nation's airports, as the commander, I was able to allow people to serve near their homes of record. They were able to spend evenings with their families and still provide full military service. We managed their schedule so that they continued to do individual soldier and airmen training with their units on drill weekends. And so there was no individual soldier or airmen skilled degradation, and their units remained fully mission ready for any combat mission that they may have been tasked by the Secretary of Defense to engage in. We were able to make adjustments for both personal and employer hardships. None of that is possible when the National Guard forces are federalized.

Mr. SAXTON. Thank you very much. Mr. Wilson, I have a couple of questions and hold them until later.

Mr. WILSON. General Rees and General Lowenberg, it is just a real honor to be here with both of you. And this has been a remarkable day, I think, in regard to the National Guard. It is National Guard appreciation and recognition day. We began early this morning with General Eberhart and his comments and his recognition of the role of the guard now and in the future. It was really heart-warming and then to know that General Bloom is his chief of staff is very helpful too, because that is from personal experience. And then to hear Secretary McHale reiterate the role of the Guard and the significance of the Guard, and particularly, General Rees, in your position with the National Guard Bureau, this has to make you feel really good and I am proud for you.

And I am grateful to be part of the Guard myself. And particularly, you know, both embody what I like about what the Guard and that is this, the positive attitude of life, and in fact, two of my sons are in the National Guard now, one field artillery and the other one in the simultaneous drill program of ROTC. Unfortunately one son has been wayward. He is an ensign in the Navy, but possibly maybe Naval Reserves sometime.

Mr. SAXTON. When his kids were little, they only had to answer one question, which service will you join?

Mr. WILSON. And I still have a 15-year-old, so he may go Air Force. But I appreciate the Guard so much and particularly in our State. For many years, when I was involved in the Guard I knew how important it was, but it actually took Hurricane Hugo to make it clear how important in natural disasters the Guard was for recovery and backing up law enforcement, not at all really a concern about posse comitatus and we are very familiar how to live with that and work with it and respect it.

But Hurricane Hugo made a tremendous difference in 1989. Then in 1991 when there was the Federal deployment for the Persian Gulf of the Air and Army Guard, there was tremendous re-

spect and has been for the Guard ever since. And it just makes me feel really good. Now another interesting point as a JAG officer, it is so much like discussing the number of angels that dance on the head of a pin. We do sit around, Mr. Chairman and discuss Title 32 and Title 10. And so I appreciate the chore. I can't wait to take this back to the real world. But these are very important issues that generally are not heavily discussed. And General Rees, could you review the advantages of keeping the National Guard forces in Title 32 status when conducting homeland security missions?

General REES. Congressman, I will go through this. I don't want to repeat what General Lowenberg said, but I think the key thing is this local control. These people know the area and know what is going on, they are close to their homes and the adjutant general has the full capacity to be able to adjust the force as necessary to deal with the situation and as a result, you cannot not only perform your functions there that need to be performed, but you can also maintain the readiness of your Title 10 expeditionary force requirements at the same time.

Mr. WILSON. And as we look to an increased role of the National Guard and Homeland Security, will that diminish the role as a Reserve to the Army and Air Force for other deployment?

General REES. Mr. Congressman, I don't believe so. I feel strongly that the adjutants general will do everything that they can to manage their force appropriately to maintain the readiness of their organizations. And I know General Lowenberg has been doing that extensively with many of the deployments that have come out of the State of Washington.

General LOWENBERG. The circumstances, if you will, the description of Guard service that Chairman Saxton mentioned in the preamble to his question, described the Guard perhaps prior to the last decade and a half, but it is certainly not a descriptor of the Guard in the last decade and a half, and I think everyone who enlists or accepts a commission in the National Guard is aware of that, fundamental commitment of patriots who are willing devote a substantial part of their lives, and their lives if necessary, to carry out the missions of the United States of America.

Mr. WILSON. General Lowenberg you are best suited as an Adjutant General (AG). Are there any impediments to National Guard forces in Title 32 status at this time?

General LOWENBERG. No impediments, Congressman Wilson. I think there are some questions about the scope and intent of 32 U.S.C. 502F which is the provision in law which provides for Title 32 service. It speaks to the authority to order members of the National Guard with or without their consent to perform training or other duties. And there are those who don't want to see the National Guard involved any more broadly than Title 32 and would question whether other duties have any meaning or whether we are simply confined to doing training only in Title 32 status. That bears policy clarification if not statutory clarification in our judgment.

Mr. WILSON. And finally, do Guardsmen in Title 32 status enjoy the same benefits and protections under the law as Title 10 counterparts.



General LOWENBERG. I might answer that initially. For pay allowances, retirement points, health care, the Title 32 benefits are exactly the same as they are for extended Title 10 duty. There are some areas like TRICARE medical benefits, access to the commissary and some space available, travel that are the same if you are performing missions in support of Operation Noble Eagle, but not if you are performing other homeland-related security missions, so there are differences at the margin.

General REES. Mr. Congressman, to emphasize a point here, we have had a number of visitations of various elements that have been called up and served all over the country post 9/11. And many times you will go into a circumstance where you have soldiers that are serving in Title 10 standing next to a soldier serving under Title 32 doing essentially the same duty and the question always comes up why don't we have the same privileges and so on. And I think if we are going to move out, and certainly take on a significant role in homeland security as currently envisioned, that this is going to have to be addressed.

Mr. WILSON. Thank you very much, and thank you again, both. I have been to a number of deployments recently, send off programs and ceremonies and I never seen the morale higher thanks to your leadership.

Mr. SAXTON. Thank you very much Mr. Wilson. Mr. Larsen of the great State of Washington.

Mr. LARSEN. Thank you, Mr. Chairman, and thank you for recognizing what we all recognize in Washington State. And I want to first apologize to General Lowenberg for not being here at the beginning of your comments, but also thank you for coming out here and providing comments to the subcommittee, and as well, to General Rees for your comments as well. General Lowenberg, I want to actually give you an opportunity to you to continue a thought that I think you started, but it is covered more completely in your testimony on page 6 with regards to this Title 10 and Title 32 issue, especially with regards to the issue we had in Blaine, Washington, and comparing the experience of getting National Guard people to the border to help with INS and Border Patrol and Customs as opposed to the issues that we had getting National Guard people to the airports in Washington State. And I think it is comparing and contrasting those. You gave us sort of the details of the upside of how well it worked on one side, but not so much about the problems we had with regards to getting deployment at the land borders after 9/11. Could you expand on that part of your testimony?

General LOWENBERG. Very happy to, Congressman. There couldn't be a starker contrast between the advantages and disadvantages of Title 10 and Title 32 for domestic deployment in support of Federal mission objectives. We responded literally within days to the airport security request. It was a totally unanticipated request from the President of the United States during a press conference and yet there was a universal spontaneous reaction throughout every State and territory to provide troops.

Quite literally, we were only delayed by having to wait for the Federal aviation agency to package a training set for our soldiers and airmen we were deploying, but we were still at 440 airports

throughout the United States within five to six days. We had up to 8,000 airmen and soldiers deployed to the airports during the holidays that year. We deployed from home station. We didn't create any new command and control structure. We didn't incur any travel expenses. We deployed from home station to duties assignments that were close to the members home of record. And they performed duties armed fully able to execute the laws of the Federal and State governments with no restrictions at all on the scope of what they could do.

And they worked, in many instances, with agencies which we already had working relationships because of the arrangements I previously described in our State. By contrast, the deployment of forces for land border security was delayed for more than 6 months and required the creation of command structure out of whole cloth and required that soldiers selected for that duty deploy to one of two mobilization stations, one on the west coast and one of the east coast, for nearly a week of training and preparation.

And once they were deployed, they could no longer train with their units, so the units from which were drawn had their mobilization readiness immediately and permanently degraded for the duration of that assignment. We were unable to make any accommodation for employer exigencies that could not be foreseen, employer emergencies. We couldn't make any personal or family accommodations for the members. And they were required to serve unarmed ostensibly to provide security against the threat of terrorist intrusion into the land mass of the United States, but they were serving unarmed.

And so as I was at the Blaine border crossing with the members of our congressional delegation, we had soldiers on duty with Border Patrol, Customs and INS, fully armed who had been working with those agencies for more than 12 years who knew one another extraordinarily well in the counterdrug program. And we had other soldiers unarmed in Title 10 duty supposedly for border security, and the comment made to the members of our congressional delegation by the senior officials of Border Patrol, Customs and INS is, the last thing in the world they expected to be confronted with was the need to protect the National Guard soldiers who had been sent in to help them.

So our assessment in our State, at least, and I don't presume to speak for all States, that border security augmentation was marginalized to a significant degree.

Mr. LARSEN. I think your testimony does provide a good compare and contrast using Title 32 and Title 10. Representing that district, you probably got one or two phone calls from my office as well as other people received phone calls. The main issue, how can we get the National Guard up there sooner rather than later, in large part because of long backups, in large part because of the extreme concern about security, fairly open border, relatively open border with Canada. So I wanted to give you a chance to talk a little bit more on the committee so we could understand what that means on the ground.

The second issue I just want to ask you about has to do with other missions. The National Guard in Washington State helps out local law enforcement with, among other things, methamphetamine

prevention and interdiction. In fact, Washington State is number three, I think, in the country in terms of States with methamphetamine interdictions. So I want to ask you about the National Guard mission with regards to the homeland defense mission and these other missions where the National Guard has been asked to step in and help out local law enforcement. Do you see some of these other nonhomeland defense missions being put on the back burner; and, if so, what might be a solution to address that?

General LOWENBERG. Congressman, I don't think we can afford to put them on the back burner. One of the things I worry about is the effort among terrorists and drug smugglers. If you want to get clandestine materials into the United States, making a pact with drug smugglers would be a very effective way of approaching that.

I think what General Rees testified to earlier was a transformational approach that takes maximum advantage of the relationships we built in the counterdrug program and doesn't abandon that program but actually embellishes it so it can be responsive to both homeland security and counterdrug needs, recognizing that those circumstances and the balance will be and should be different in every State and territory.

Mr. LARSEN. Thank you very much.

Thank you, Mr. Chairman.

Mr. SAXTON. Thank you.

One of the questions that we always like to ask is what you need that we might be able to provide in order to enable you to better carry out your mission. We have got, you know, lots of demands on our resources, but we need to know what your priorities are for things that you need. You need detection equipment. You need communications equipment. You need better command and control. If you had a wish list, what would be on your wish list for us to try to provide for you?

General LOWENBERG. Well, speaking for the adjutants general, Mr. Chairman, at the top of our wish would be a recognition statutorily and in regulation of the role of the proper National Guard Bureau being our channel of communications with the senior players beyond the Secretaries of the Army and the Air Force. I have been very specific in my written remarks about what regulatory and statutory changes would be involved with that. That—it just cannot be overstated the importance of that effective channel of communications, uninhibited channel of communications between the military forces of the several States and the senior policymakers in the Department of Defense. That would be very high on the list.

Mr. SAXTON. Explain to me the current situation and how you would like to see it changed.

General LOWENBERG. Currently, by statute, the National Guard Bureau is the channel of communications between several States and the Secretaries and Chiefs of Staff of the Army and the Air Force. But, literally, there is no statutory authority to be a spokesperson or a channel of communications between the States and anyone above, if you will, in the DOD hierarchy, the Secretaries of those two respective services.

So we think it is quite important, for example, that the law recognize that the Chief of the National Guard Bureau be able to be our channel of communications with Secretary McHale and with the action agent at the joint staff.

Mr. SAXTON. And other Federal agencies, FEMA?

General LOWENBERG. I think it is appropriate to recognize that we have avenues of access to FEMA within the Department of Homeland Security and other agencies, but within military channels that is where we need to have the clarification.

Mr. SAXTON. General Rees.

General REES. Sir, I would say there were several things that were alluded to here about training, equipment and so on that need to be addressed; and certainly we can provide you with more information on that. It is very clear that the importance of Mr. McHale and General Eberhardt in defining the mission and establishing what the standards are and the expectations are will be critical for us to be able to identify what we can do at the State level.

Certainly when it comes to the operations of the National Guard in a joint effort before immediate response, many of the things that we normally get through the Army and Air Force channels are not necessarily the missions that are going to correlate to this homeland security requirement. So the integrated priority list of General Eberhardt will be very critical to us, and the mission described by Mr. McHale will be paramount.

I would say there is another area that you demonstrated a very intense interest in, was the intelligence area. We think that there is a huge potential here for the National Guard to provide fusion between State and local and the national requirements of the Department of Defense within proper bounds.

Mr. SAXTON. Could you expand on that?

General REES. As you know here, General Lowenberg is the head of State Emergency Management, has extensive relationship throughout his State government. The typical adjutant general has the same capabilities. So they are going to have a situation of national awareness of what is going on in their State in relationship to other emergency agencies, to law enforcement, et cetera. They are going to be capable of providing information to the Guard Bureau and to Northern Command about the situation as it may exist in a certain State and could be a conduit for passing that information back from Northern Command to State and local authorities as appropriate.

Mr. SAXTON. So the flow of information both ways from the local level to the higher command level and back from information agencies in the Federal Government to the local level.

General REES. That is correct.

General LOWENBERG. We are participating, Mr. Chairman, in an advanced concept technology demonstration project in our State and a 5-year accelerated, funded program that would create an IT architecture that would create seamless integration from the incident commander to General Eberhardt at Northern Command. So, again, the National Guard utilizing our Guard net, IT systems, our distance technology training point programs and the advanced concept technology demonstration, if it proves to be what we all hope it will be, will provide General Eberhardt extraordinary situational



awareness of the threat conditions and the potential need for Federal military forces to augment emergency responders in every State and territory.

Mr. SAXTON. You will be pleased to know that DOD personnel have been on the Hill here within the last ten days seeking support for them to put up a pilot program with that system here in the D.C. area.

General LOWENBERG. We are participating with the State of Louisiana and State of Virginia. We had that equipment placed in our Military Joint Operation Center and our State Civilian Emergency Operation Center and in local jurisdiction Emergency Operation Center. So that program is well on its way.

Mr. SAXTON. One final question, on the Civilian Support Team (CST) teams and Congress intent, I think it was last year—last year or the year before, Congressman Taylor sponsored an amendment which was successful in a House markup which became law, as you know, requiring the 50 States to stand up or requiring CST teams to be stood up in the 50 States. My recollection is—in fact, this is more than my recollection. This is, the person or staffer who wrote the amendment provided for us to fund that, and we are anxious to do so, but we required a plan from the Department of Defense, which to my knowledge we haven't received yet.

General REES. Mr. Chairman, it is my understanding that that is still being worked on. They are working to meet your requirement. The latest version of it that I have seen indicates that they were to start in fiscal 2005 with a program that would take about 18 to 24 months to stand up to the rest of these teams.

Mr. SAXTON. Do you know when you anticipate that we may see it?

General REES. The latest version that I had heard about was perhaps around the first of June.

Mr. SAXTON. We will be marking up in April, won't we? I wonder if you could pass along the urgency of the situation. We are going to be marking up our bill in April, and I don't know when the Senate is going to mark it up. It would be nice if we had it in time to look at it and understand it before April. We are anxious to get this done, and we want to do it right. We want to provide the resources that are needed for the deal according to some plan, and we would like to see it.

General REES. Mr. Chairman, we would be happy to take that message back to the individuals in the office that are responsible for putting that report together.

Mr. SAXTON. Mr. Larsen.

Listen, thank you for the job that you do. Thank you for being here today. Your message was clear and articulate, and we appreciate it very much.

We hope you will pass the word back to the folks—your colleagues that you work with around this country, the members of this committee and the full committee and the Congress of the United States appreciate very much the job that the Guard has done and the degree of flexibility that you have shown and commitment that you have shown over the last months and particularly since September of 2001. Thank you for being here. We have en-

joyed it and benefitted from it and I hope the country has as well.  
Thank you very much.

[Whereupon, at 4:45 p.m., the subcommittee was adjourned.]

---

---

# **A P P E N D I X**

MARCH 13, 2003

---

---





---

---

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

**MARCH 13, 2003**

---

---



**Statement of Chairman Jim Saxton  
Subcommittee on Terrorism, Unconventional Threats and  
Capabilities**

---

**Subcommittee Hearing on Department of Defense Force Protection**

**Policy**

---

**March 13, 2003**

**Chairman:** Gavel down. Brings meeting to order.

[Makes the following statement.]

The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this afternoon for the first time in formal session. Although we have had several informal meetings and briefings, today marks the first public hearing of this important new body, which I am honored to lead in conjunction with our distinguished ranking member, Marty Meehan of Massachusetts, and our vice chairman, Robin Hayes of North Carolina. As I've said in private, but now want to put on the record, I thank all the members who have volunteered to serve on this subcommittee, and look forward to working with all of you as together,

we help the Department of Defense and the military services to fight the scourge of terrorism.

I have proposed and my colleagues support an active agenda, as there is much to be done. Despite the ever-growing nature of the terrorist threat at home and abroad which culminated with the tragic events of September 11th, the Armed Services Committee has never before established a standing committee to address the many issues involved. It is our duty to be diligent, and very diligent we will be, while recognizing that we cannot accomplish everything immediately, despite our collective sense of urgency.

Our first hearing is a fitting start. We not only begin with the general view of the Department of Defense, which is logical, but there is an interesting contrast of the old and new in the distinguished positions our witnesses hold. Let me explain.

Our first witness, the Honorable Paul McHale, while a gentleman of extraordinary abilities, experience, and common sense, occupies a brand new senior policy making office in the Department of Defense. He is the Assistant Secretary of Defense for Homeland Defense and is testifying today for the first time in that capacity. As part of his responsibilities, he will help to oversee the work of the Department's



newest combatant command, Northern Command, whose commander testified before the full committee earlier today. Both Secretary McHale and General Eberhart, in turn, are under the nurturing, but watchful eye of this body, the newest standing committee concerned about force protection and homeland defense. That's the new part of this equation I referred to earlier.

Now to the old, at least in lineage—I find great comfort in the fact that an enduring institution of this great country, indeed, the institution that fought for our freedom before we were a nation, is in the forefront of the effort. I'm talking about the national guard, or militia as it was known in the revolution. The guard was there at our nation's birth and continues to perform critical duties in protecting our homeland. Yes, we have some technical questions about how the missions will be performed, and we will address those. But I first wanted to recognize the fundamental and continuing importance of the national guard to American freedom and ideals.

This is the first of a series of hearings we will conduct before our markup in late April, and it sets the stage for those that follow. Our objective today is to begin to get an understanding of the issues that face the Department of Defense as it commences its coordination efforts with the new Department of Homeland Security, in an attempt to learn how

we can help the process, either legislatively or through the budget. Secretary McHale, I don't think you will get a more open invitation of support during your tenure, and we certainly look forward to renewing our friendship and working with you.

**Chairman:** Yields to Mr. Meehan for any opening remarks he may wish to make.

**Mr. Meehan:** Makes opening remarks.

**Chairman:** [Makes the following statement.]

We have two panels of witnesses for our proceedings this afternoon. I want to welcome our first witness who is:

- The Honorable Paul McHale, Assistant Secretary of Defense for Homeland Defense

As I noted in my opening remarks, Paul McHale is not only a former member of Congress, but also a distinguished former member of the Armed Services Committee. We are pleased that he is serving in his new capacity and welcome his testimony.

At the outset, I will state that, without objection, your prepared statement will be entered into the record. Mr. Secretary, please proceed.

**Witness:** Makes opening statement.

**Chairman:** Yields to Mr. Meehan for the purpose of asking questions of the witnesses.

Statement by

Mr. Paul McHale,

Assistant Secretary of Defense for Homeland Defense

Before the 108<sup>th</sup> Congress

House Subcommittee on Terrorism, Unconventional Threats and Capabilities

U.S. House of Representatives

March 13, 2003



## Introduction

Mr. Chairman and Members of the Committee: I appreciate the opportunity to meet with you on the critical subject of our nation's security.

As the President said, on the eve of the standup of the new Department of Homeland Security, "The world changed on September the 11th, 2001. We learned that a threat that gathers on the other side of the earth can strike our own cities and kill our own citizens. It's an important lesson; one we must never forget. Oceans no longer protect America from the dangers of this world. We're protected by daily vigilance at home. And we will be protected by resolute and decisive action against threats abroad."

"We're tracking down terrorists who hate America, one by one. We're on the hunt. We [have] them on the run. And it's a matter of time before they learn the meaning of American justice. We're opposing terror regimes that are arming with weapons of mass destruction to threaten the peace and freedom of this world. And we're taking unprecedented measures to defend the homeland with the largest reorganization of our government in more than a half a century."

At home and abroad, the Department of Defense is a significant contributor in this national effort to secure our nation and its people.

The Department is prosecuting the war on terrorism abroad. The President understands that a terrorist can attack at any time, at any place, using any conceivable technique. He also understands that it is physically impossible to defend against every conceivable threat in every place, at every time.

To successfully defend against terrorism, and other 21<sup>st</sup> century threats, requires that we take the war to the enemy. And the task of the Department is to put pressure on

terrorists wherever they are, in Afghanistan, across the globe, to ensure that they have no safe haven, no sanctuary.

With respect to the war abroad, U.S. military forces, when directed by the President, are charged with engaging terrorist forces and the governments or other entities that harbor them. In this effort, the Department works closely with other government agencies, including the departments of State, Treasury, and Justice, and the intelligence community.

At home, all elements of society have a crucial stake in reducing our vulnerability to terrorism; and all have highly valuable roles to play. Protecting our nation requires an unprecedented level of cooperation throughout all levels of government – with private industry and institutions, and with the American people. The federal government has the crucial task of fostering a collaborative environment, and enabling all of these entities to work together to provide the security our nation requires. The new Department of Homeland Security is tasked with the responsibility of leading this national effort to protect our nation against terrorist attacks.

At home, the Department of Defense plays a valuable role in securing our nation as well and the Secretary of Defense has made a public commitment to work closely with the new Department of Homeland Security in order to coordinate our respective responsibilities.

However, before discussing further the Department's role in helping secure our nation and its people at home, it is important to distinguish the differences between homeland security and homeland defense.

### **Homeland Defense and Homeland Security**

As described by the President in the National Strategy for Homeland Security, **homeland security** is defined as a concerted national effort to prevent terrorist attacks within the United States, reduce the vulnerability of the United States to terrorism, and minimize the damage and assist in the recovery from terrorist attacks.

On the other hand, the Defense Department defines **homeland defense** as the military protection of United States territory, domestic population, and critical defense infrastructure against external threats and aggression. It also includes routine, steady state activities designed to deter aggressors and to prepare U.S. military forces for action if deterrence fails.

With respect to homeland security, the Defense Department will operate in support of a lead federal agency. While in homeland defense activities, the Defense Department will take the lead and be supported by other federal agencies. In fact, Section 876 of Public Law 107-296, the Homeland Security Act of 2002, recognizes the Department of Defense's lead role in the conduct of traditional military missions by providing that "[n]othing in this Act shall confer upon the Secretary [of Homeland Security] any authority to engage in warfighting, the military defense of the United States, or other military activities, nor shall anything in this Act limit the existing authority of the Department of Defense or the Armed Forces to engage in warfighting, the military defense of the United States, or other military activities." This section clearly delineates the difference between homeland defense activities and homeland security activities – a precision that will be important to keep in our minds and to articulate clearly to the American public.

#### **The Department of Defense's Role in the Security of the Nation**

In his testimony before Congress in May of last year, the Secretary of Defense described three distinct circumstances in which the Department of Defense would be involved in activities within the United States:

The first case was **extraordinary circumstances**, which require the Department to execute its traditional military missions. For example, combat air patrols and maritime defense operations. In these cases the Department plays the lead role and is supported by other Federal agencies. As in the case of combat air patrols where the Federal Aviation Administration provides data to assist the efforts of Air Force fighter pilots in identifying and, if necessary, intercepting suspicious or hostile aircraft.

Also included in the category of extraordinary circumstances are cases in which the President, exercising his Constitutional authority as Commander in Chief, authorizes military action. This inherent Constitutional authority may be used in cases, such as a terrorist attack, where normal measures are insufficient to carry out Federal functions.

The second case was **emergency circumstances** of a catastrophic nature—for example: responding to an attack or assisting in response to forest fires, floods, hurricanes, tornados and so forth, during which the Department may be asked to act quickly to provide or to supply capabilities that other agencies do not have.

Finally, the Secretary noted **temporary circumstances**, where the Department is given missions or assignments that are limited in duration or scope and other agencies have the lead from the outset. An example of this would be security at a special event like the Olympics. Another example is assisting other Federal agencies in developing capabilities to detect chemical/biological threats.



Subsequent to the Secretary's testimony, three significant changes to the Department of Defense have fostered an evolving perspective of our role at home in the security of our nation.

First, the Secretary of Defense, with the approval of the President, changed the Unified Command Plan and stood up, on October 1, 2002, the **U.S. Northern Command**. U.S. Northern Command's mission is to:

- Conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility; and
- As directed by the President or Secretary of Defense, provide military assistance to civil authorities including incidence management operations.

U.S. Northern Command's area of responsibility includes air, land and sea approaches and encompasses the continental United States, Alaska, Canada, Mexico, and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico, Puerto Rico and the U.S. Virgin Islands. The defense of Hawaii and our territories and possessions in the Pacific remain the responsibility of U.S. Pacific Command. U.S. Northern Command will additionally be responsible for security cooperation and coordination with Canada and Mexico.

In addition to defending the nation, U.S. Northern Command will provide military assistance to civil authorities in accordance with U.S. laws and as directed by the President or Secretary of Defense. Military assistance is always in support of a lead federal agency, such as the Department of Homeland Security.

Military civil support includes domestic disaster relief operations that occur during fires, hurricanes, floods, and earthquakes. Support also includes counter-drug operations and consequence management assistance, such as would occur after a terrorist event employing a weapon of mass destruction.

Second, the Fiscal Year 2003 National Defense Authorization Act directed the establishment of an **"Assistant Secretary of Defense for Homeland Defense."** I am honored and thankful to have been nominated by the President and confirmed by the Senate to serve as the first Assistant Secretary of Defense for Homeland Defense.

In accordance with Section 902 of Public Law 107-314, the Bob Stump National Defense Authorization Act of 2003, my principal duty is "the overall supervision of the homeland defense activities of the Department of Defense." My charge, as given to me by law, by the Secretary of Defense, and by the President is to lead and focus the Department's activities in homeland defense and homeland security, ensure internal coordination of DoD policy direction, provide guidance to Northern Command for its homeland defense mission and its military activities in support of homeland security, to include support to civil authorities, and to coordinate with the Homeland Security Council (HSC), the National Security Council (NSC), the Department of Homeland Security (DHS), and other government agencies. In layman's terms, I am responsible for recommending to the Secretary the roadmap and the "rules of the road" for the Defense Department's future role in securing our nation at home.

Third, the Fiscal Year 2003 National Defense Authorization Act also directed the establishment of an **"Under Secretary of Defense for Intelligence."**

The Under Secretary of Defense for Intelligence will have the primary responsibilities to assure that the senior leadership of the Department and Combatant

Commanders receive the warning, actionable intelligence and counter-intelligence support needed to pursue the objectives of our new defense strategy.

The Under Secretary will also enhance Defense Department intelligence-related activities, provide a single point of contact for coordination of national and military intelligence activities with the Community Management Staff and strengthen the relationship between the Secretary of Defense and the Director of Central Intelligence. So, in terms of this forum, the new Under Secretary will define and provide oversight for the Defense Department's participation in national Indications and Warning.

### **The National Guard's Role in the Security of the Nation**

One of the critical elements in DoD's contribution to the security of our nation is the National Guard. Since the terrorist attacks of September the 11<sup>th</sup>, the Defense Department has depended so much on the National Guard that many of our accomplishments at home and abroad would not be possible without them.

In fact, on September 11, 2001, members of the 102nd Fighter Wing, Massachusetts Air National Guard at Otis ANGB, led the first military response to the terrible attack on America. Two F-15 Eagle jets from Otis arrived at the World Trade Center, just minutes after United Airlines Flight 175 sliced into the second tower. While they were unable to alter the course of history on that morning, they stood guard with renewed vigilance. They were the first, but they were not the last.

Clearly, because of where they are located in their relationship to state governments, the National Guard is one of the absolutely critical elements in developing the military's role in responding to attacks on the United States, and that includes response to mass casualty attacks. That is why, of course, that it is no accident that General Eberhart, who is the commander of the new Northern Command has as his chief

of staff a National Guard general. His links into the National Guard are absolutely critical.

The National Guard is quite capable of conducting selected homeland defense missions, such as the Air National Guard's important role in continental air defense. However, the National Guard is also combat ready to conduct overseas military operations and is relied upon by combatant commanders as part of a strategic reserve.

In the past, the National Guard was dual-tasked. In wartime, the nation has expected the Guard to go fulfill its mission overseas; in peacetime, the nation has expected the Guard to be available for domestic emergencies. The terrorist attacks of September the 11<sup>th</sup>, have now taught us that the National Guard may be called upon to do both at the same time, not by accident but because our nation's enemies may attack us in both places at once.

Consequently, as DoD reviews how best to deal with the challenge of the new security environment, it is mindful of the need to properly balance the application of the total force to: defend the homeland, contribute to the global war on terrorism, meet military commitments abroad, and, if necessary, participate in a major theater war.

In general, the National Guard can support homeland security in several ways. First, the Guard can operate in state service under the direction of the governors. For example, on September 11, the National Guard of New York, New Jersey and Connecticut responded to the attacks on the World Trade Center.

Second, in state service but performing duties of federal interest, in Title 32 status.

Third, in federal service, in Title 10 status, for example when the National Guard is mobilized to serve under the direction of the President or the Secretary of Defense.



The Commander of Northern Command will have authority over the Guard only when it is serving in a Title 10 status. Otherwise, although he can set training and readiness standards for Guard units when they operate in Title 10 status, command authority over the Guard's activities would remain with State governors.

These arrangements have worked well in the past. The challenge today is to translate them into our new security environment. There are many proposals for doing so, and we'll work with the NSC, HSC, DHS, Congress, and the governors to make certain that we have an approach that meets the nation's needs.

### **The Department of Defense-Department of Homeland Security Relationship**

March the 1<sup>st</sup> marked an historic day for the federal government. Over 170,000 employees from more than 20 different agencies officially became part of the Department of Homeland Security, creating a more effective, organized and united defense of our homeland. The Department of Homeland Security is a vital and important step in reorganizing our government to meet the threats of a new era as we continue the work of securing our nation.

The Secretary of Defense has made a public commitment to work closely with the new Department of Homeland Security in order to coordinate the respective responsibilities. DoD and DHS have complementary missions and capabilities. In general, the Department of Defense is responsible for **homeland defense** missions – to defend the land, maritime, and aerospace approaches from external threats – while the Department of Homeland Security will be responsible for major elements of domestic security and civil preparedness. DoD will also provide military assistance to U.S. civil authorities in accordance with U.S. law, as directed by the President and the Secretary of Defense. For example, such assistance could include support for incidence management operations led by the Department of Homeland Security when authorized by the President

or the Secretary of Defense. There will be an ongoing requirement for U.S. Northern Command to coordinate plans, exercises and training with the operating components of DHS.

As the Assistant Secretary of Defense for Homeland Defense, I will supervise all DoD homeland defense activities, including combatant command capabilities, and will coordinate all requests for assistance and cooperative ventures between the Department of Defense and the Department of Homeland Security.

### **Conclusion**

In conclusion, the departments and agencies charged with U.S. national security share a common goal: to assure the security of American citizens, territory, and sovereignty. DoD and DHS have complementary missions and we welcome DHS as a partner. As always, America's men and women in uniform stand ready to defend the nation at home and abroad.

Thank you, Mr. Chairman.

FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE HOUSE ARMED SERVICES  
COMMITTEE, SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS  
AND CAPABILITIES

STATEMENT OF

MAJOR GENERAL RAYMOND F. REES, USA

ACTING CHIEF, NATIONAL GUARD BUREAU

BEFORE THE HOUSE ARMED SERVICES COMMITTEE, SUBCOMMITTEE ON  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES  
MARCH 13, 2003

FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE HOUSE ARMED SERVICES  
COMMITTEE, SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS  
AND CAPABILITIES

Good morning, Mr. Chairman and other distinguished members of this committee. Thank you for the invitation to testify before you today on the role of the National Guard in the important homeland security mission.

#### Recent and Current Activities.

As we begin the 21st century, Homeland Security is the most important issue facing the United States. For almost 200 years the continental US was not directly attacked (with the minor exception of Japanese coastal shelling and incendiary balloons), until the terrorist attacks of the 1990s and on September 11<sup>th</sup>, 2001. We now believe the prospect of future attacks is significant. To better defend the US, the government has mobilized its resources and has undertaken a major reorganization to more effectively meet the challenge. While the National Guard performed superbly in response to the attacks of September 11, 2001, we have begun to make changes to better respond to future attacks, and we will need the help of the Department of Defense and the Congress to make some of those changes.

The National Guard has a significant role in Homeland Security. Just as the active force is the first to deploy in support of US operations abroad, the National Guard is the first military force to deploy in support of most Homeland Security requirements. The National Guard is a unique dual status, citizen-soldier force that can be activated by the Governor in support of state emergencies and also can be federalized to support national contingency requirements. The Governor can employ the National Guard under state active duty (state commanded, state financed) and Title 32 (state commanded, federally financed), or the National Guard can be federalized under the provisions of Title 10, (federally commanded, federally financed). Its dual state-federal status makes the National Guard a cost effective, flexible force that can be deployed in a variety of circumstances. Like the Guard units in the states, the National Guard Bureau (a Title 10 entity) has dual roles. We communicate policy, requirements and situational awareness information in both directions through the federal-to-state channel. Further, because most of the state Adjutants General are also the emergency manager for their state, and because many are also their state's Homeland Security Director, we are involved in intergovernmental issues, as well as federal military and interagency ones.

This dual-mission, multi-faceted capability of the Guard was demonstrated in the aftermath of September 11th.

Immediately after the attack on September 11, the National Guard responded. National Guard air assets took to the skies to secure our airspace and other forces were quickly sent to the World Trade Center and the Pentagon to assist with security and recovery efforts. Soon after, the President asked the Governors to secure critical US airports and they responded by deploying Guardsmen in Title 32 status at airports in a matter of hours. In addition, many of the states' governors ordered their Guardsmen, in State Active Duty status, to secure critical infrastructure facilities, such as bridges, nuclear power plants, and federal buildings, throughout their states and many of those missions continue today. Other National Guard units and personnel were activated under Title 10



to augment security at the US borders. Their mission was to support the Department of Justice and the Department of the Treasury in ensuring that commerce continued to flow while our vital interests were protected. These homeland security missions and others were conducted, and some have continued to be conducted, while Army and Air National Guard forces have been deployed for peacekeeping and stabilization actions in the Balkans and elsewhere, and as a critical part of the war in Southwest Asia. The Guard has also been mobilized to perform force protection missions in the United States in support of preparation for possible war with Iraq. As expected, the National Guard has conducted and continues to conduct all missions in an exceptional manner.

As we move forward, it is apparent that the National Guard will be increasingly involved in all aspects of the Homeland Security mission. The Homeland Security areas we focus on include:

- Combating terrorism
- Military Assistance to Civilian Authorities
- Responding to chemical, biological, radiological, nuclear and high-yield explosives incidents
- Missile Defense
- Critical Infrastructure Protection
- Information Operations
- Force Protection
- Protecting the Nation's Sovereignty.

In addition to these mission areas, the National Guard Bureau's recently-established Office of Homeland Defense will facilitate military support to civil authorities by the Army and Air National Guard. Military support to civil authorities includes domestic disaster relief operations that occur during fires, hurricanes, floods, and earthquakes. Our support also includes counter-drug operations and incident management assistance, such as would occur after a terrorist event employing a weapon of mass destruction. The National Guard Bureau, in addition to our statutory role as the channel of communication between the Army and the Air Force and the National Guard of the several states, has coordinated with the Combatant Commander of U.S. Northern Command to perform that same role. As part of this, the National Guard Bureau provides situational awareness on state-commanded National Guard operations to the Commander of U.S. Northern Command to augment his ability to effectively plan for and manage the overall role of his command.

## The Future of the National Guard in Homeland Security

The fight against terrorism and the protection of our homeland is expected to be a protracted endeavor much like the Cold War. To that end, many policy experts, reports, and studies have advocated an expanded role for the National Guard in Homeland Security. While some have suggested that the National Guard should be reoriented, reequipped, and retrained for the Homeland Security mission, the reality is that the National Guard is an integral part of the Army and Air Force Total Force mission capability and that role is vital to the survival of the nation. In the past the resources, personnel, equipment and training provided for the wartime mission were sufficient to allow the National Guard to also fulfill its local and state support role by responding to local disasters and military support to civilian authorities. Times have changed, however. The threat posed by well-financed, sophisticated and determined international terrorist groups has raised the bar as to what the National Guard must be able to do. While the National Guard will continue to maintain a high state of readiness for overseas operations, it must also better prepare itself to respond to the Homeland Security mission within the US, the District of Columbia, Puerto Rico, and the US possessions and territories. To that end, we are working hard to find ways to meet the increased demands of the Homeland Security mission while still maintaining our ability to execute our Total Force requirements.

The increased threat and global proliferation of ballistic missiles poses a significant threat to the US, our deployed forces, and our allies. In response to this threat, in December 2002 the Department of Defense directed the deployment of an effective missile defense system capable of defending the territory of the United States against limited ballistic missile attack. The Army National Guard accepted the mission to man the Army portion of the Ground-based Midcourse Defense (GMD) system, including both operational and security force elements. The GMD segment is the cornerstone of the Ballistic Missile Defense System Test Bed, and will have an Initial Defensive Operations (ID)) capability by September 2004. This high-visibility program, which will provide protection against limited ballistic missile attack, is an example of the evolving role of the National Guard in Homeland Defense.

Over the next year, and as much longer as it takes, the National Guard Bureau will take the lead in improving the posture of the National Guard for its homeland security mission.

The National Guard Bureau will work with the States as they perform a mission area analysis to determine what additional capabilities are needed to accomplish the homeland security mission and will utilize a systematic programmed approach designed to build our Homeland Security posture for the future. These are the features of that program:

- Consolidate the Homeland Security requirements of the 50 States, territories and the District of Columbia. (States know the actual operational requirements better than anyone).

- Validate these requirements at the National Guard Bureau level and craft them into packages for submission to the appropriate Combatant Commanders, to the Army and Air Force as requirements that can be built into programs for funding, and to the Assistant Secretary of Defense for Homeland Defense.  
Use the same requirements to attract emerging funds as appropriate from other government agencies and from any supplemental funding that might occur.
- Use our developed requirements to advise and educate agencies, offices, commands, and leaders that have an interest in supporting Homeland Security.
- From valid requirements we will build funded programs that insure the success of Homeland Security by using a systematic long-term approach. We believe that a long-term approach is needed to help insure a sustained, comprehensive protective posture for our nation.

As part of this requirements process, which may identify new needs – and thus possibly requests for new manpower or equipment resources, the National Guard Bureau will work to ensure that all feasible efforts are made to leverage technology that improves our Homeland Security capabilities and with it, improve our overall protective posture.

The road ahead also includes a transformation of National Guard Counter Drug efforts into an integrated Counter Narcotics/Homeland Defense Counter Terrorism program. These mission areas employ many of the same tactics, techniques and procedures, as well as equipment, training and skills. Therefore, a great deal of cross-skill transfer will begin immediately once the change is effected, and a quick, effective, seamless transition between and across mission sets will allow Guard troops to readily take their places on the front lines of the war against terrorism at home and abroad.

#### Northern Command and the Department of Homeland Security.

Our government has initiated a massive reorganization to better respond to the Homeland Security challenge. Northern Command has been activated, the new Department of Homeland Security is in the process of being organized, and the Department of Defense has created a position of Assistant Secretary of Defense for Homeland Defense. The National Guard Bureau will work with the Assistant Secretary for Homeland Defense and Northern Command to insure that National Guard missions and capabilities are fully integrated into the overall plan for Homeland Security. Specifically, it will assist Northern Command as that command moves from an initial operating capability to a full operating capability by:

- Providing situational awareness of activities by the National Guard of the several states (the non-federalized National Guard).
- Integrating and synchronizing existing plans.  
Coordinating National Guard resource and training requirements.
- Facilitating communication between Northern Command and the State Adjutants General.
- Augmenting the Northern Command staff with National Guardsmen.

Northern Command will undergo a critical year as it transitions from an initial operating capability to a full operating capability by October 2003. During the coming year, the National Guard will be providing personnel to Northern Command in order to fill critical personnel requirements. Additionally, the National Guard is working to develop situational awareness for Northern Command as to the activities that affect Homeland Security within the 50 states and territories. Although most activities of incident management at the federal level will fall under the control of the Department of Homeland Security, a constant monitoring of state-level activities and interests is needed by Northern Command in order to support the lead federal agency when needed. The National Guard, through the National Guard Bureau, is the natural conduit for DoD elements to the states and territories on military-related matters. The majority of the states use the Adjutant General of that state as the state emergency manager. The National Guard is intimately involved in all activities of Homeland Security at the state level. The National Guard Bureau is actively pursuing discussions and several initiatives within the Department of Defense which will likely result in better exploitation by all segments of the Department of Defense of the Bureau's capability as a two-way channel of communication to the National Guard of the several states. We are excited about assisting Northern Command in its emerging role and look forward to facilitating federally funded support of state activities.

In addition, the National Guard Bureau will work, through the Assistant Secretary of Defense for Homeland Defense, with the new Department of Homeland Security to insure that the National Guard's capabilities and requirements are fully integrated in the overall Homeland Security plan. The new Department of Homeland Security will be greatly assisted by the National Guard plans that are already in effect in all of the states and territories. Since the vast majority of homeland security activities come under state and municipal or other local control, the National Guard planning and activities under State Active Duty (state controlled and funded) and under Title 32 (state controlled, federally funded) will be an integral part of the processes being crafted by the new Department. National Guard Training Centers are existing assets that can be economically expanded to support realistic training and exercises with first responders, law enforcement agencies, and all levels of government integrating National Guard capabilities in homeland security roles. Several states have initiated pilot programs for this effort with federal support at the request of Congress. The National Guard is taking an open supportive approach to intradepartmental, interagency and intergovernmental cooperation for the defense of our Homeland. We each must succeed for all to succeed.

The Army National Guard and the Air National Guard bring several inherent strengths to the Homeland Security environment. Aside from a capable, trained and organized force, there is also an in-place information technology infrastructure that has the potential to provide an efficient, reliable, interoperable, and user-friendly channel of communications for the Office of the Secretary of Defense and Northern Command through the National Guard Bureau to the Army and Air Guard. The present information technology infrastructure provides a robust reach-down capability to Army and Air Guard units in

the states. However, to meet the emerging needs of Homeland Security missions, enhancements in network reliability and security will have to be incorporated. Additionally, the new requirements pose new challenges in areas such as wireless technology that will allow direct command, control and communications with on-site responders. The National Guard Bureau is uniquely positioned to provide this coordinated, controlled capability, consistent with the statutory requirements of Title 10.

The National Guard supports any overseas fight primarily by supporting Army and Air Force initiatives. Most programmatic and force structure actions, therefore, are Service specific, supporting either the Air War or the Ground War through the respective Services. Examples of initiatives underway in this area include the Army National Guard Restructuring Initiative, an initiative to replace a portion of the existing heavy and light combat structure with Mobile Light Brigades prepared for full spectrum operations in support of the new defense strategy. This will meet the Army's evolving needs for expeditionary warfare, as well as giving us more Guard forces well-suited to Homeland Security tasks in support of US Northern Command and US Pacific Command. In the Air National Guard, a Transformation Initiative will result in capabilities-based forces with improved Intelligence, Surveillance and Reconnaissance, Information Technology, Medical Service and operational aircraft with the ability to make strong contributions to both aspects of the Guard's dual federal-state mission. As we render Homeland Security support to the Lead Federal Agencies, however, we must change our approach and support them as a Joint Force – not two separate Services. The lead agencies need and want to deal with a single entity within the National Guard and this year we are prepared to provide that in a seamless manner. A Joint Staff approach out of the National Guard Bureau will present a single flow of information and will strive for a single funding line to support operations. In addition, the State Area Command will become a true joint state headquarters with enhanced capabilities. In this way, our team is coming together to support our communities and homeland institutions with expanded capabilities and improved linkages to national command and control mechanisms. In addition, the National Guard will continue to participate in the planning and execution of interagency exercises with local, state and federal agencies thereby building relationships that may prove useful during future contingency operations.

The ability of the National Guard Bureau to maintain awareness, conduct coordination, provide guidance and resources to the National Guard must be strong to meet the growing needs of Homeland Security. To that end, the National Guard Bureau's Office of Homeland Defense has evolved as the focal point for that effort. It has assumed responsibility for these initiatives. To further ensure continuity and centralized management of all Homeland Security activities, our Office of Homeland Defense recently incorporated the civil support function under its control. The NGB Office of Homeland Defense will work with the States to determine their requirements to accomplish the Homeland Security mission. It will be this entity within the National Guard Bureau that will coordinate with the States, The Joint Staff, U.S. Northern Command, U.S. Pacific Command, and, through the Office of the Secretary of Defense, with other federal government agencies to manage all Homeland Security efforts.



### The Civil Support Team Program.

For the past two years the National Guard has had a very tangible asset to offer in support of the civilian and emergency first responder communities in the area of Homeland Security - its Civil Support Teams. With the help of Congress, the Department of Defense, and the Army, the Guard has continued to strengthen the Civil Support Program, under which these teams fall. The teams provide rapid support to local, state and federal authorities in dealing with the consequences of chemical, biological, radiological, nuclear or high yield explosive events. Of the 32 Civil Support Teams that have been established, the Secretary of Defense has operationally certified 30. The remaining two are expected to be certified no later than March 31, 2003. An additional 23 teams have been authorized by the Congress, and DoD is developing a plan to field them as expeditiously as possible.

Several of the certified teams were integrally involved in response efforts to the September 11th terrorist attack and to the anthrax attacks and hoaxes that were perpetrated throughout the nation in the ensuing months. The Civil Support Teams have been increasingly integrated into the planning, training and operations at every level of emergency response ever since. In fact, during the year following the September 11th attacks, the 27 certified teams collectively performed nearly 800 missions at the request of the agencies they support.

These teams provide state and local authorities specialized expertise and technical assistance to the incident commander to:

- Identify chemical, biological, radiological, nuclear or high yield explosive substances or agents.
  - Assess the situation; determine the type of weapon used and the likely consequences.
- Advise the incident commander on potential courses of action.  
Assist the local incident commander's response strategy with cutting edge technology and expertise.

Operationally, these teams are under the command and control of the governors through their respective Adjutants General in a USC Title 32 status. Should it be required, a team can be federalized and called to serve in a USC Title 10 capacity. The National Guard Bureau provides logistical support, standardized operational procedures and operational coordination to facilitate the employment of these teams and to provide depth and backup capability to states currently without a full-time Civil Support Team.

In order to be the best resource possible to those entities they assist, it is crucial that the teams continue to be complementary to and interoperable with all of the federal, state and local organizations with whom they work. This means that they must continue to be equipped with and trained on the state of the art technologies, requiring that they remain a high priority for resourcing at all levels within the Department of Defense.

Issues of importance that are being addressed at many levels in support of improving the Civil Support Team program include the following: coordination with Transportation Command and other commands to formalize the processes of requesting airlift for these units. This is required to minimize response times to remote and/or hard to access incident sites and thereby optimizing their utility to incident commanders. Intensive recruiting, special pay and acquisition issues are being worked by staff at the National Guard Bureau's Homeland Defense Office to address some of the more challenging issues the program faces in remaining a value-added capability to their civilian counterparts.

#### The National Guard – A Total Force Component with A Key Homeland Security Role

In summary, Mr. Chairman and distinguished members of the committee, our adversaries will not rest—“the clock is ticking”—so our preparation must be immediate, exact and effective. The National Guard gives this nation a tremendous capability in that its members live, work and play within the communities they defend. The Guardsmen know their home turf. The people trust their National Guard and always feel comforted by their presence during a crisis. We will take that trust and solid experience to build the National Guard into a proactive, technologically superior team that is trained and ready to deal with any and all threats to our homeland. To further that end, the National Guard Bureau will remain the best link from the DoD to the National Guard of the several states. Because of the dual roles of the Guard, this link will address departmental, interagency, and intergovernmental policy and requirements issues. The NGB, and the Guard as a whole, will continue to cooperate and train with all local, state and federal agencies in an effort to improve response capabilities. In its dual State and Federal roles, the National Guard will continue to provide ready forces to the combatant commanders, we will support other government agencies when asked, and will take the lead, when appropriate, in the defense of our homeland.

It has been my distinct pleasure to be here today. I thank you for the opportunity to testify on this critically important aspect and mission of the National Guard. I welcome any questions you may have.

FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE HOUSE ARMED SERVICES  
COMMITTEE, SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES

**STATEMENT OF**

**Major General Timothy J. Lowenberg, Adjutant General, State of Washington and  
Chair, Homeland Security, Adjutants General Association of the United States  
(AGAUS)**

**BEFORE THE HOUSE ARMED SERVICES COMMITTEE, SUBCOMMITTEE ON TERRORISM,  
UNCONVENTIONAL THREATS AND CAPABILITIES  
MARCH 13, 2003**

FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE HOUSE ARMED SERVICES  
COMMITTEE, SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES

Good afternoon, Mr. Chairman and members of the Committee. For the record, my name is Major General Tim Lowenberg. I am the Adjutant General of the State of Washington and Chair of Homeland Security for the Adjutants General Association of the United States (AGAUS).

Thank you for the opportunity to address the role of the National Guard, in combination with other uniformed service components, in providing for homeland security and homeland defense. In this time of expanding terrorist threats and limited fiscal resources, we must take maximum advantage of everything the National Guard and other components of the Department of Defense can contribute to our collective security.

I am one of a majority of Adjutants General who have homeland security responsibilities significantly transcending conventional command and control of Army and Air National Guard forces. I am "dual hatted" (to use the military vernacular) as our state's senior emergency management official. The state Emergency Management Director, Mr. Glen Woodbury (who also serves as the current President of the National Emergency Management Association [NEMA]) works directly for me as head of the one of the three major divisions of the State Military Department. I am advised and supported in this capacity by Mr. Woodbury and by a State Emergency Management Council (EMC) consisting of representatives of cities, counties, sheriffs, state and local police chiefs, fire chiefs, local emergency management directors, health officials, ecology officials, fire protection bureau officials, building trades officials, seismic safety experts, search and rescue volunteers, and private sector business leaders. I meet with this group of state and local leaders at least once every 60 days, and more often as needed.

In 1999, at the behest of Governor Gary Locke, our state also formed a Committee on Terrorism (COT) which reports to me through the Emergency Management Council. Presidential Decision Directive 63 (PDD 63), with which you are all familiar, prompted our formation of the state Committee on Terrorism. PDD 63, along with the early work of the U.S. Commission on National Security/21<sup>st</sup> Century (the so-called "Hart-Rudman Commission") convinced us that our nation was entering a new and decidedly dangerous period; one marked by increased vulnerability to domestic terrorist attacks. Although it would be nearly two more years before the fatal attacks of September 11, 2001, we were well aware that our national interests had been under attack by Al-Qaida since at least 1991. We therefore formed the Committee on Terrorism in the fall of 1999. That investment in multi-jurisdiction collaboration and coalition building has paid off handsomely as we've dealt with the challenges of the post-9/11 world. The Committee on Terrorism is our fusion point for marshalling the efforts of more than thirty (30) federal, state, and local government agencies and private sector organizations. The full committee operates through more than a dozen standing subcommittees and work groups which report through the EMC to the Adjutant General and the Governor.

I am also responsible for overseeing our state-wide Enhanced 911 program – everything from managing E-911 tax revenues to assuring essential system upgrades and support for local public safety answering points (PSAP's). In this capacity, I'm assisted by a 27-member

Advisory Council of government and private sector leaders, including representatives from the private sector wire-line and wireless communications industry.

Following the attacks of September 11, 2001 Governor Locke also directed that the Adjutant General serve as the state Homeland Security Advisor. In that capacity, I am our state's primary point of contact with the White House, the Department of Homeland Security and the National Governors Association on all matters pertaining to homeland security. In that role, I also chair the weekly meetings and oversee the daily liaison of the state Domestic Security Executive Group, which includes the governor's chief of staff and senior policy advisors, several other key cabinet officials and our separately elected state Attorney General.

I am submitting a diagram, for the record, depicting these multiple responsibilities [Atch 1]. I've taken the liberty of doing so for several reasons: first, because these multiple roles are not unique to me or to our state – a majority of the nation's Adjutants General have similar dual civil-military roles and responsibilities; second, these duties do not conform to the position description or range of homeland security responsibilities of any senior military leaders outside the National Guard – no other active duty or reserve component general officers deal so extensively and habitually with senior federal, state, local and private sector civilian emergency responders; and third, these duties underscore the unique capabilities of Adjutants General as forward deployed military commanders for purposes of executing federal and state emergency response plans.

### Th National Guard

Just as the role of the Adjutants General is unique, so too is the composition and constitutional status of the Army and Air National Guard forces we command. When discussing the National Guard, it must be understood that the "Guard" is really two separate and distinct organizations. The terms of art used to describe these two organizations are the National Guard of the several States and the National Guard of the United States. The National Guards of the several states are state military organizations maintained by the sovereign states under the Militia Clause of the U.S. Constitution. These National Guard forces can be used at the direction of the Governor at state expense and for state purposes (e.g., state active duty deployments in response to natural disasters such as flooding and wild fires) or at federal expense and for federal purposes (e.g., guarding our nation's airports).

Article 1, Section 8 of the U.S. Constitution expressly authorizes states to provide military support to the federal government "to execute the laws of the union, suppress insurrections and repel invasions". Under Title 32, United States Code (T32, USC) National Guard members have been used at federal expense and "*in the service of the United States*" to train the traditional, part-time force, for counter-drug support for federal, state and local law enforcement agencies, for providing Civil Support Team assistance to federal, state and local emergency responders, and, most notably, for augmenting airport security following the attacks of September 11, 2001. The third and final National Guard status is as the National Guard "*of the United States*"; this legally distinct status refers to the reserve components of the United States Army and Air Force under the provisions of Title 10, United States Code, sections 3062 (c) (1) and 8062 (d). Unlike state active duty and Title 32 duty, Governors and Adjutants General have no command or control over National Guard Forces that have been ordered to Title 10 federal duty; National Guardsmen/women become indistinguishable members of the federal armed forces upon being placed on Title 10 orders.

The various Guard statuses and the expansive range of potential Title 32 duty are depicted in the diagram marked as Attachment 2.

As a result of these distinct legal statuses, all National Guard members are commissioned or enlisted in each of two separate and legally distinct military organizations: the National Guard of the individual state and the National Guard of the United States. The Supreme

Court recognized these important status distinctions in Perpich v. Department of Defense, 496 U.S. 334 (1990), a case in which the Court analogized that National Guard members have three hats in their closet: a civilian hat, a state militia hat and a federal reserve of the Army or Air Force hat, only one of which can be worn at any given time.

It has been my experience that most active duty military leaders and many supposedly knowledgeable commentators don't understand these distinctions and therefore adopt the simplistic view that the National Guard is available only in state active duty status or as a Title 10, federally-controlled force. This overlooks the broad range of Title 32 duty status options in which the National Guard can be used under state control but at federal expense and for federal purposes. In truth, as I will explain momentarily, use of the National Guard in Title 32



status offers federal authorities an operationally and fiscally superior range of options for undertaking homeland defense and homeland security missions.

For ease of reference, I will use the term "National Guard" throughout the balance of my testimony to mean the National Guard under state control in either State Active Duty or Title 32 status. When referring to the National Guard of the United States (the Guard's Title 10 reserve component status), I will call attention to that special context.

### **The National Guard Bureau**

The Adjutant General is the commander of all Army and Air National Guard units in his state, regardless of his branch of service. The Adjutant General therefore exercises joint command. What then is the Chief of the National Guard Bureau (CNGB)? It might surprise you to learn that he is *not* the commander of the National Guard "of the United States", the federal component of the National Guard; in fact, the National Guard of the United States does not have a national command structure. Rather, the National Guard Bureau is a "channel of communications" between the Departments of the Army and Air Force and the several states (10 USC 10501) and the Chief is the head of the Bureau, not a commander. The responsibilities of the CNGB are articulated in 10 USC Sections 10501-10507, the National Guard Bureau Charter from the Secretaries of the Army and the Air Force, and other DoD directives and regulations. Foremost among these is the Chief's role as senior spokesman between the Army and Air Force and the states on all matters pertaining to the National Guard. In addition, the CNGB is responsible for insuring that the National Guard of the several states is prepared to respond to Military Support to Civil Authorities (MSCA) and other state mission requirements while concurrently training and otherwise preparing for mobilization as the primary reserve of the Army and Air Force (i.e. as the National Guard of the United States<sup>1</sup>).

### **The National Guard of the Several States**

The governors of the several states routinely employ the National Guard in a traditional Military Support to Civil Authorities (MSCA) role and in concert with other state resources when responding to state and local emergencies. They employ their National Guard forces in state active duty status and at state expense before requesting federal assistance through their state emergency management functions to DHS/FEMA. They can also obtain assets, including other National Guard forces, from other states using one of several emergency assistance compacts (for example, the Emergency Management Assistance Compact [EMAC] which now has 47 state members) or by direct, ad hoc agreement with other states.

When state-to-state mutual assistance is provided in response to an emergency for which there has been a Presidential Disaster Declaration, the expenses of the supported state,

<sup>1</sup> National Guard Bureau Charter and DoDD 3025.1

including the costs of assistance from supporting states, are reimbursable under the Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121 *et. seq.* This highlights an important new dimension in the war on terrorism. As part of our national homeland security planning, we need to recognize that National Guard military assistance for civil authorities and other National Guard functions (both intra and interstate assistance) can be funded through FEMA and need not be funded solely through the Department of Defense.

Governors and Adjutants General have a great deal of experience dealing with major disasters. The State of Washington, for example, has averaged at least one Presidential Disaster Declaration each year for the past forty (40) years. Many of these disasters have

required activation of the National Guard. For us, Military Support to Civil Authorities is not a theoretical mission possibility that might occur once during a 2 or 3 year military assignment; it is the kind of bread and butter emergency response mission to which we devote a substantial portion of our careers.

Most recently, National Guard Weapons of Mass Destruction Civil Support Teams (CSTs) were deployed from supporting states to assist supported states in recovering potentially dangerous NASA Space Shuttle debris. In furnishing this Title 32 assistance, the supporting states continued to exercise command and control over the deployed CSTs, with tactical supervision being extended to the supported state(s). The supporting teams were also deployed under the Emergency Management Assistance Compact, rather than through normal DoD channels. This illustrates the flexibility of using existing state National Guard command channels to furnish Title 32 National Guard assistance to states struck by major disasters.

Adjutants General manage the readiness and operations of their state Army and Air National Guard forces pursuant to guidance from their Governor and from the CNGB acting on behalf of the Office of the Secretary of Defense (OSD) and the Army and Air Force. They do so through a state command element called the State Area Command (STARC). The STARC is an Army National Guard unit augmented by appropriate Air Guard personnel to achieve a measure of "jointness". The STARC, which can itself be mobilized under Title 10 USC, can be used to execute state active duty, Title 32 and/or Title 10 USC functions in carrying out MSCA missions and wartime readiness and mobilization missions. The STARC provides mature, cost-efficient state command and control of National Guard forces regardless of the nature or purpose of their mission.

I used our STARC to mobilize, deploy and oversee the operations of soldiers and airmen in state active duty status when quelling the World Trade Organization Conference riots in Seattle in 1999. I used the STARC to mobilize, deploy and oversee the operations of soldiers and airmen in Title 32 federal pay status when rushing to augment airport security following the attacks of September 11, 2001. I am also using the STARC to mobilize and deploy soldiers for Title 10 active duty in support of Operations Noble Eagle and Enduring Freedom. The STARC's MSCA responsibilities are described in detail in DoD Directive 3025.1 (MSCA), paragraphs 4f, 6c and 7e.

The operational and fiscal advantages of using the Guard in Title 32 status and in fully utilizing the existing STARC command structure are best illustrated by two post-9/11 missions. Shortly after the attacks of 9/11, President Bush called upon governors to make National Guard forces available to guard the nation's airports. His request came without forewarning during a presidential press conference. Notwithstanding these unusual circumstances, within 24 hours of the President's request approximately 1,000 Guardsmen deployed to key airports. The FAA and NGB developed a five-day train up program. Over 6,000 Guardsmen were then trained and deployed to 440 airports. During the peak holiday season in 2001, over 8,000 Guardsmen were deployed to our nation's airports.

The airport security mission was a classic case of the National Guard being used "in the service of the United States" for a federal purpose and at federal expense. Although the terms of the Title 32 deployment and rules of engagement were specified by the federal government (the supported jurisdiction), command and control of the uniformed forces remained with state military authorities (the supporting jurisdictions). The states used their existing STARC and subordinate command headquarters to mobilize and manage the deployed forces. No new command structures had to be created. No extraordinary mobilization expenses were incurred. Because the soldiers and airmen remained under state command and control, they trained at home station and soldier and employer hardships could

be accommodated by rotating personnel in and out of the Title 32 mission. Work schedules were carefully managed so that soldiers and airmen continued to drill with their units. They thereby maintained individual and unit war-fighting proficiencies, assuring their continued readiness for OCONUS combat missions. Most importantly, if the soldiers' primary unit had been needed for an OCONUS combat, combat support or combat service support mission, we could have rotated other soldiers into the airports and returned the affected soldiers to their units for OCONUS deployment.

By contrast, when Border Patrol, Customs and INS needed augmentation to assure the security of our nation's land borders, federal authorities insisted that National Guard members be federalized in Title 10 status. This required costly and cumbersome federal command structures to be created from scratch. Instead of training at home station, all soldiers had to ship out to one of two federal mobilization stations. Instead of operating under familiar state command structures, command was exercised by an active duty Army headquarters on the opposite coast. Once on Title 10 orders, the soldiers could no longer train with their units. Over the course of their six month border deployment, they were no longer available for OCONUS combat duty, individual soldier skills eroded and the combat readiness of their original units of assignment was irreversibly compromised. Moreover, in contrast to the speedy deployment of National Guard forces to the nation's airports (3 to 6 days), imposition of these cumbersome and costly federal control procedures delayed deployment to the borders for more than six (6) months. To add insult to injury, National Guard soldiers had to be deployed unarmed in order to comply with the Posse Comitatus Act restrictions on Title 10 forces, thereby minimizing their effectiveness as border security augmentees. As a result, at the border crossing at Blaine, Washington armed Title 32 Washington National Guard soldiers assisted Border Patrol, Customs and INS agents with counter-drug operations as we have done for more than twelve (12 years) while unarmed, federalized National Guard soldiers from many of the same units had to be protected by Border Patrol, Customs and INS agents at the same border while they performed marginally effective counter-terrorism duties.

The Adjutants General of the United States and the nation's governors are adamant that when National Guard forces are used domestically they should remain under state control, whether operating for a state purpose (at state expense and under state control) or for a federal purpose (at federal expense but under continued state control under Title 32, USC). The nation's governors, by formal resolution adopted at their mid-winter conference on February 25, 2003, have called upon federal authorities to use the National Guard in Title 32 status instead of Title 10 for all domestic missions. A copy of the Governors' resolutions on *Army and Air National Guard Policy and Terrorism and Homeland Security Policy* are attached to these remarks [Alchs 3 and 4].

### **Dual Missioning**

The Phase III Report of the U.S. Commission on National Security / 21<sup>st</sup> Century (February 15, 2001) argued for "orders-of-magnitude improvements in planning, coordination, and

exercises. The government must also be prepared to use effectively – albeit with all proper safeguards – the extensive resources of the Department of Defense. This will necessitate new priorities for the U.S. armed forces and particularly, in our view, for the National Guard".

With that assessment in mind, the Commission recommended to Congress that the National Guard "should:

Participate in and initiate, where necessary, state, local and regional planning for responding to a WMD incident

- Train and help organize local first responders

- Maintain up-to-date inventories of military resources and equipment available in the area on short notice
- Plan for rapid inter-state support and reinforcement; and
- Develop an overseas capability for international humanitarian assistance and disaster relief."

The Adjutants General concur with the Commission's assessment and recommendations, having been assured by Commission representatives that the Commission did not intend for the Guard to be turned into a constabulary force or to assume homeland security missions in lieu of existing combat, combat support and combat service support missions. The Commission recognized, as we do, that we are able to perform our domestic support roles so well precisely *because* of our OCONUS combat training and experience.

The Adjutants General Association of the United States (AGAUS) and the National Guard Association of the United States (NGAUS) urge the President to direct the Secretary of Defense, and request the Congress where necessary, to authorize, support, equip and fund the National Guard to assume significant homeland security responsibilities. These responsibilities must be recognized as an important mission but not the sole or primary mission of the National Guard. Although there may be a need for selected units and personnel to be specially missioned or resourced for these purposes (e.g., CSTs and recently proposed Homeland Security units – see S. 215), homeland security can most effectively and efficiently be accomplished as a *dual mission* that compliments, enhances and draws its essential strength from the National Guard's continued combat force structure, training and experience.

In truth, we are already doing as much as possible to support the activities recommended by the Hart-Rudman Commission. We are constrained from doing more, however, because the recommendations do not fall within the wartime missions for which we are currently funded. S. 215 (currently pending before the Senate Committee on Armed Forces) would substantially advance the recommendations of the Hart-Rudman Commission by authorizing the National Guard to perform federally approved MSCA missions pursuant to a formal Governor's Plan for Homeland Security. The proposed program is patterned after the counter-drug program model in which each state administers a program of full-time National Guard counter-drug support for civil agencies. Within prescribed national guidelines enforced by the National Guard Bureau, the Governor's Homeland Security Plan would marshal National Guard resources to meet the unique homeland security needs of each state and territory.

The Adjutants General Association and the National Guard Association of the United States strongly support S.215 and urge its adoption by both houses of Congress. We believe the road ahead should also include an integrated Counter Narcotics / Homeland Defense Counter Terrorism program, drawing upon the existing authorization of the counter drug program and the new homeland security authorization of S.215.

### Civil Support Teams

The Secretary of Defense has certified 31 of the 32 currently authorized and funded Civil Support Teams as being fully mission ready. The remaining team should be certified no later than 31 March 2003. The 107<sup>th</sup> Congress authorized a total of 55 teams but did not provide funding for the additional teams. The Hart-Rudman report for the Council on Foreign Relations urges Congress authorize and fund 66 teams. The National Emergency Management Association (NEMA), the International Association of Emergency Managers (IAEM), the Council of State Governments (CSG), the National Governors Association (NGA)



and the National Guard Association of the United States (NGAUS) join the Adjutants General Association of the United States (AGAUS) in urging Congress to authorize and fund at least one (1) CST in every state and territory. To do any less is to treat every man, woman and child in 23 of our states and territories as acceptable casualty risks

As the Adjutant General of the first CST to be certified to Congress as fully mission ready, I am intimately familiar with the operational capabilities and limitations of these teams. Their capabilities are truly unique – there is nothing else like them. They provide a critical margin of safety for emergency responders and citizens at large. They also provide a critical base of information for officials charged with protecting the public's safety. Our teams provide invaluable training and exercise support to civilian emergency responders, routinely integrating such responders into our training scenarios. We have even deployed civilian responders as part of our CST to such national special security events as the 2002 Winter Olympics. The limitations of the teams are largely confined to time and distance factors over which we have little control. Although our entire team can deploy on a single C-17 and we regularly practice such deployments, there is no dedicated tactical airlift for any of the CSTs. The only sure method of employment is to drive to the disaster scene. Our teams are on a 2-hour 24/7 response line, but the harsh reality is that weather and traffic conditions make it impossible to provide timely support to remote areas in several states or to the states and regions that don't have their own CST. On more than one occasion, we have had to decline requests for deployment of our team to sensitive out-of-state events because we couldn't get military airlift.

The CST program needs two things: first, every state and territory needs at least one Civil Support Team and, second, we need a plan for the military airlift of the teams. This latter need is especially critical in the event of asymmetric terrorist attacks.

#### **A New Concept**

CNGB was recently recognized as the channel of communications between the Commander, NORTHCOM and the National Guard of the several states. As a member of the General Officer Work Group at NORTHCOM, I join my fellow Adjutants General in applauding this development. For nearly sixty years, combatant commanders and Service Secretaries have communicated with the several states through the National Guard Bureau. It is the Bureau that coordinates and facilitates multi-state responses to complex domestic and foreign emergencies. The Bureau is a one-stop-shop for the Department of Defense in dealing with the several states, territories and the District of Columbia. CNGB should play the same role not only with Commander, NORTHCOM but with all other civilian and military officials involved in executing our national homeland security strategy. The CNGB should, for example, have a similar formal relationship with the new Assistant Secretary of Defense for Homeland Defense and the new MSCA action agent (The Joint Staff). The CNGB should serve as the channel of communications between them and the states for National Guard matters. As part of this relationship, the NGB would sustain a 24/7 situational awareness of

National Guard state active duty and Title 32 operations and provide a daily current operational picture to all concerned organizations.

NGB can easily provide this service by utilizing existing and upgraded information capabilities such as \*GUARDNET, Reserve Components Automation System (RCAS), electronically linked Information technology classrooms, the GCCS/SIPRNET, and federally provided tactical systems.

#### **The Concept at the Operational Level**



A guiding principle of this concept is that federal missions executed by the states should be federally funded and subject to federal oversight. The CNGB assists OSD and the Services in performing this oversight function across the entire spectrum of National Guard missions. Utilizing Title 32 as an operational status, as well as a training status, is a transformational force application of the National Guard and is within the scope of 32 U.S.C. Section 502(f). Some OSD officials have argued that Title 32 can only be used for training and not for operational missions. As a lawyer and law school professor, as well as a military commander, I respectfully take exception to their narrow interpretation of Congressional intent. 32 USC 502 (f) authorizes the Service Secretaries, with or without consent of the member, to order soldiers and airmen "to perform training or other duty..." (emphasis added). The first tenet of statutory construction is that statutes are to be interpreted in a way that gives meaning to all words and phrases. The stilted definition embraced by those who are hostile to Title 32 operations renders the phrase "or other duties" meaningless. To be intellectually honest, they would also have to argue that the President's use of the National Guard for airport security was patently illegal; the most they will say, however, is that the President's actions were "legally problematic". The fact is that Title 32 has been used repeatedly in recent years for purposes as diverse as counter drug support, Civil Support Team assistance and securing our nation's airports.

Adjutants General, through their STARC headquarters, provide the Command, Control and Communications (C3) for National Guard units serving in Title 32 and State Active Duty (SAD) status. Presently, the states are transitioning from separate and distinct Army National Guard and Air National Guard state headquarters to a joint headquarters command structure (the Joint State Headquarters, JSHQ). Most states will have transitioned to the JSHQ by December 2003.

JSHQ could also be mobilized under Title 10 (in whole or in part) and, in that status, exercise C3 of units from any component serving in Title 10 status. The JSHQ will coordinate, through its director of military support (DOMS), with the state emergency management office and the NGB. By working with State Emergency Preparedness Liaison Officers (SEPLOs) [SEPLOs are reserve component Title 10 officers - normally colonels or Navy captains] and the use of joint task-organized forces, the JSHQs will create a capability for immediate joint state-level response.

#### **Th Concept at the Tactical Level**

The question that must be answered is, "If the National Guard is deployed operationally under Title 32 while federal (Title 10) military forces are operating in the same geographic area for generally the same purpose, can there be unity of effort without unity of command?" The answer, in the judgment of the nation's Adjutants General, is an unqualified "Yes". The Federal Response Plan itself presumes willing collaboration and unity of effort toward a common objective from local, state and federal civil and military agencies. Unity of effort and

coordination of command, rather than unity of command, has worked well in responding to emergencies and disasters of every imaginable scope and magnitude.

The recent local, state and federal Shuttle COLUMBIA response and recovery effort provides a real world illustration. Local sheriffs and fire departments provided the immediate response forces. A patch-quilt of federal military and non-military elements responded. The Texas and Louisiana National Guard happened to be in a Title 32 training status that weekend. The National Guard of those two states deployed to provide security forces within hours of notification of the disaster. They were deployed by order of their Adjutants General. Immediately, NORAD, through 1st Air Force, as CONR, diverted two (2) Texas Air National Guard F15s, in Title 32 status, to provide aerial recon capabilities. These Title 32 aircrews

supported the Title 10 headquarters without regard for "command" technicalities or clarification of court martial authority. An Alabama Air National Guard KC-135 tanker was placed in Title 10 status to provide aerial refueling capabilities. The Texas and Louisiana Civil Support Teams were deployed by their Governors to provide immediate response to a hazardous material incident of the magnitude of a "weapon of mass destruction" scenario.

The National Guard units in Texas transitioned seamlessly from Title 32 status to State Active Duty (SAD) status on Monday, 3 February 2003. Those forces (approximately 500 personnel) were then commanded or controlled by an Army National Guard lieutenant colonel; the forces consisted of Texas Army National Guard in state active duty status as well as Oklahoma, Arkansas and New Mexico Army and Air National Guardsmen in Title 32 status (the WMD-CSTs). The task force commander provided daily situational awareness reports to the National Guard Bureau, and those reports were routinely passed on to DOMS and Northern Command. The National Guard forces were "working for" the following state and federal civilian agencies: EPA, NASA, Texas Emergency Preparedness Department and FEMA, each of which also had their own tactical assets committed (first responders/emergency responders, technical subject matter experts, and the like). The federal military elements performed their role as tasked by the Defense Coordinating Officer (DCO) provided by 5th US Army. This response clearly illustrates a federal/state/local civil/military emergency response in which unity of effort was coordinated primarily by the Texas State Emergency Management Agency without either a deliberately-developed ad hoc operations plan or unity of "command" in the military Title 10 sense. The result was a timely, efficient and wholly effective outcome.

The designation of Quick Reaction Forces/Rapid Reaction Forces (QRF/RRF) presents yet another opportunity to use this transformational approach in meeting the federal portion of the Homeland Defense mission. Use of Title 32 National Guard forces would provide DoD and the Combatant Commanders the flexibility of meeting their tactical and operational requirements without formally mobilizing National Guard forces. The states can organize, train, and employ appropriately sized forces based on DoD/Combatant Commander-approved criteria and can most effectively and efficiently do so in Title 32 status. These forces, if required, can even be placed in Title 10 status for limited periods to achieve unity of command under NORTHCOM or PACOM. This concept of operations is based on the time-tested First Air Force model in which National Guard forces seamlessly transition from Title 32 to Title 10 status and then back to Title 32 status, as necessary to achieve mission objectives.

Conversion of the current National Guard Counter Drug effort provides another transformational opportunity. Approximately 3,000 National Guardsmen serving in Title 32 ADSW status are engaged in counter drug activities. Many of these activities are fully supportive of and closely aligned with needed Homeland Defense missions. Integrating Counter Drug personnel and assets with a Governor's National Guard Homeland Security Plan (S. 215) would substantially enhance our nation's homeland security strategy.

Other opportunities exist for using this same transformational approach in such areas as National Guard medical assistance in CBRNE incidents, surveying critical infrastructure, and distributing the National Stockpile. NGB has developed a joint requirements identification and validation process and has input from 40 of the 54 states and territories. As these requirements are further refined, more opportunities will be identified to meet DoD and DHS operational requirements.

## **The Way Ahead**

AGAUS has been advised that the Acting Chief, National Guard Bureau (ACNGB) has met with the reserve component chiefs, under NORTHCOM auspices, and there is support for the National Guard providing the initial Homeland Defense and Civil Support capability for OSD. In the event Title 10 assistance from other reserve or active components is required, they could be prepared to provide necessary follow-on forces. A revision of the EPLO program to provide more deliberate use of local Reserve units through expanded planning, exercises, and pre-approved immediate response should also be part of this homeland security enhancement strategy.

Notwithstanding the support of these other service components, the National Guard of the several states and the NGB remain the best link for DoD and NORTHCOM for military support to state and local civil authorities. In furtherance of this role, creation of a JSHQ, in a form supportable by the Adjutants General, should be a high priority for DoD and NGB.

Several legislative, policy and cultural challenges need to be effected to make these transformational strategies a reality. The first and most fundamental cultural change is to correct the misperception by some OSD and Service staff members that the only way to meet a national requirement with National Guard forces is to "federalize" or mobilize the Guard in Title 10 status. As the nation's governors and Adjutants General have emphasized, however, our homeland security and homeland defense strategies are most dramatically advanced by taking maximum advantage of the domestic use of the National Guard in Title 32 status.

The most urgently needed legislative and policy changes are:

- Establish the Chief, National Guard Bureau as the channel of communications between the National Guard of the several states and the new MSCA/Civil Support executive agent for DoD (the Assistant Secretary of Defense, Homeland Defense) and the new action agent for DoD (the Joint Staff DOMS)
- Amend DoD Directives 3025.1 and 3025.15 to reflect these new relationships and operational concepts
- Amend 10 USC Sections 10501-10503 to reflect these new relationships.
- Acknowledge that 32 USC Section 502(f) provides for use of the National Guard of the several States "in the service of the United States" and provide the necessary regulatory guidance or, if necessary, amend the United States Code with more explicit provisions authorizing the operational use of the National Guard in Title 32 status
- Include in NORTHCOM / PACOM Integrated Priority Lists validated National Guard requirements for Homeland Security

Provide policy and resource support to merge separate state-level Army and Air National Guard headquarters into a Joint State Headquarters (JSHQ) in each state.

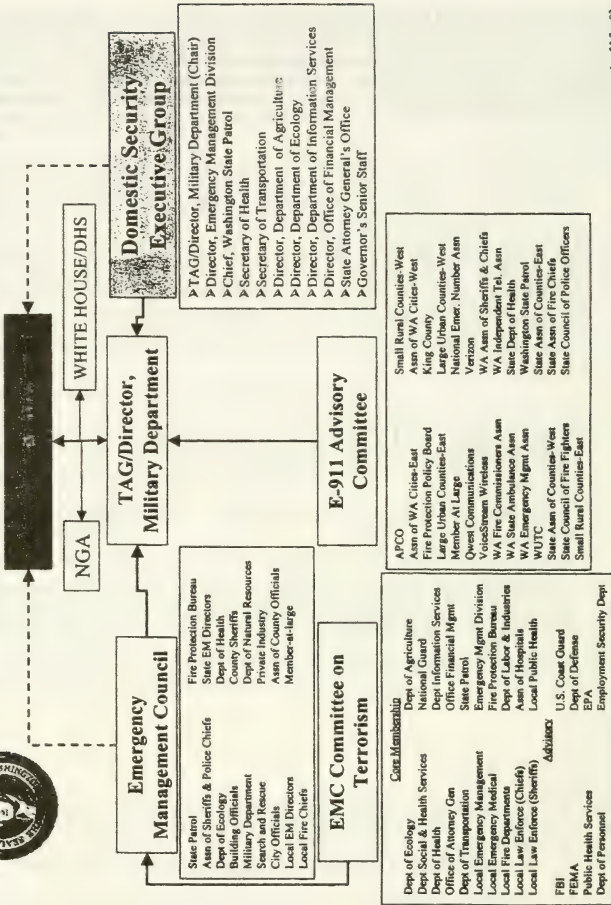
Provide policy and resource support for upgrades to National Guard administrative and operational communications/IT capabilities, both classified and unclassified.

Coordinate transformation of the National Guard Counter Drug program into an integrated Counter Narcotics / Homeland Security / Homeland Defense counter terrorism program.

In conclusion, I would like to thank the Committee for this opportunity to convey the thoughts and concerns of the nation's Adjutants General and of our Governors. We are soldiers and airmen who are devoted to freedom's cause and to our nation's security. The first step in this long journey is to capitalize on the transformational capabilities and established forward presence of the National Guard. Working with other elements of the Department of Defense and civilian emergency responders, we can, we must, and we will protect our homeland and win the global war on terrorism.



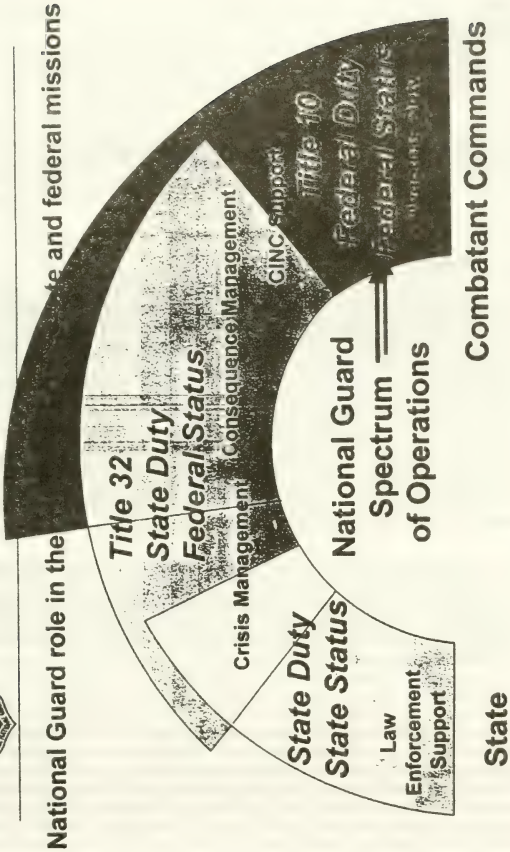
# Washington State Domestic Security Infrastructure







# National Guard: A civil/military, state/federal organization *by design!*





## **HR-6. Army and Air National Guard Policy**

### **6.1 Preamble**

Just as the federal government's relationship to all other aspects of state and territorial activity has matured and become institutionalized over the years, so has the state, territorial, and federal role of the National Guard ripened into a stable and eminently sensible system for living up to the letter and spirit of the U.S. Constitution against a backdrop of the variety and the special characteristics that mark each of the states of the Union. Because the size of the active military has been reduced so dramatically while its requirements have not, the role of the National Guard as the foremost "reserve of the Army and the Air Force" has become so powerful and significant, that it is sometimes forgotten that the Guard, in peacetime, is under the command of the Governors; and that the Guard is the only military force that a Governor has available in time of disasters and emergencies. The states and territories have an enormous stake in the ongoing effectiveness and efficiency of their National Guard.

NGA notes that national defense strategy requires the Army and Air National Guard to be capable of fighting with the active forces. In keeping with the "Total Forces Policy," many active units cannot enter into combat as effective units unless accompanied by mobilized elements of the National Guard. The National Guard must be properly equipped, efficiently trained, and fully staffed to meet these responsibilities.

### **6.2 Training**

NGA supports annual training exercises of National Guard units. However, the requirements for training and military education should be consistent with the needs of the military force, and should recognize the serious responsibility to members of the Guard as "citizen soldiers," to their families, to their employers, and to their communities. This should be kept in mind when developing the right mix of monthly and annual training exercises for the Guard. An exception to this might be expected in the special training of certain units, but this must be the exception and not the rule, and on a voluntary basis.

We ask the employers of National Guard men and women to recognize their need to be away during times of training or when activated by the Governor or federal authorities. The services that they perform enhance all of our lives.

### 6.3 Control of the Guard

The Governors wish to emphasize that, unless activated in federal service, the National Guard is under state control with Governors as commanders-in-chief. We call attention to the U.S. Constitution, Article I, Section 8, clause 16, which enables Congress:

to provide for organizing, arming, and disciplining the militia, and for governing such part of them as may be employed in the service of the United States, reserving to the states respectively, the appointment of the officers, and the authority of training the militia according to the discipline prescribed by Congress...

Subsequently, Congress enacted Title 32 of the United States Code (USC), which affirms the Governor's control over the National Guard in peacetime without any restraints such as those pertaining to the Posse Comitatus Act. Under Title 32 of the USC, the nation's Governors are clearly in command and control of the National Guard in their respective states and territories. Congress likewise enacted a separate Title 10 of the USC, which is focused primarily on the active military to deal with war and national crises. In this instance, the Guard can be activated as a part of the regular forces under the command of the President of the United States. The Governors believe when the National Guard members perform domestic missions they should do so in Title 32 USC status rather than Title 10 USC status, unless the President has called them in Title 10 for a federal mission requiring federal troops, such as to repel an invasion. In Title 32 status, National Guard members can continue to train with their regular units and in times of federal mobilization these Guard members are available to deploy with their units. This is not the case if individual National Guard members were in Title 10 status, where they would not be available for deployment with their unit. The Governors further note that Title 32 status for domestic deployments avoids all posse comitatus issues.

### 6.4 Training and Equipment

NGA commends the Army and the Air Force for the efforts that are being made to enhance training and to better equip the National Guard in recognition of its vital contribution to our national defense. Although the National Guard is better equipped now than ever before in its history, it is still under equipped. Many states and territories are currently experiencing equipment shortages in critical mission areas such as tactical fixed wing airlift and utility helicopters. Such shortages could critically affect our readiness. The Army's current aviation modernization plan fails to adequately address this shortage and we urge Congress and the Administration to ensure an increased supply of helicopters for the Army National Guard. The National Guard is still lacking in the area of modernization, but a great effort has been made, and continues to be made, to ensure that units that will deploy early in the stages of any future mobilization are being provided with support on the same basis as active units that deploy early.

Full-Time Support (FTS) remains the number-one readiness priority for the National Guard across the country. Modest increases to the Guard's total obligation authority have been made by recent congressional actions. However, these gains in congressionally authorized FTS levels are not sufficient to sustain the National Guard.

From the days of the militia to the present, the National Guard reflects the genius of our system of government. In the evolution since colonial days, through the revolutionary war era, through the wrenching experience of the civil war, it has been an instrument through which citizens voluntarily made their contribution to the common defense of their land, their values, and their heritage.

The Total Forces Policy restored the Guard to its more traditional place in the nation's defense strategy. NGA believes that a strong National Guard, which the President can mobilize in time of national crisis, serves to remind friend and foe of our national commitment to freedom and to the system of government for which we are famous and even envied.

Today's active forces, constrained in size and scope by the enormous cost of personnel and material, must rely on National Guard augmentation. Realizing that approximately one-half of the defense budget is attributed to personnel cost, the guard, which receives only a fraction of a month's pay, represents a most cost-effective way to protect our national security and provide for a professionally trained and committed Army and Air Force for the defense of the nation.

The nation's Governors are proud that the National Guard is able and capable of performing tasks in the interest of national defense and security, and is available at their command to assist the citizens of the states and territories, should the need arise.

### **6.5 Reorganizing and Restructuring of Military Forces**

Changes in the national security environment and the arms negotiations have caused the U.S. Department of Defense to evaluate force structure in light of budgetary constraints.

Governors believe that military force reductions prorated across the entire military structure may not be the most cost-effective means of achieving a strong national defense. Moving structure from the active military components into the National Guard could achieve budget savings while continuing to protect the nation's vital interests. Historically, our nation has relied on the National Guard as a mobilization base. National Guard units have achieved high readiness levels, providing a real mobilization asset to support global missions on short notice. Most units, including examples such as military police, Army and Air Guard air defense, tactical air units, and air transportation units, provide excellent immediate capability for lower peacetime operating costs than active service units.

The Governors remain committed to a National Guard that provides the Governors of the states and territories with sufficient forces that have the organic chains of command, equipment, and capabilities necessary to meet the federal and state missions of the nation. Analyses accomplished almost a decade ago established that a 405,000-force structure is the minimum prudent number to meet that objective, and the Governors have consistently supported that number. The events of September 11, 2001, have caused a broad reevaluation of the entire spectrum of terrorism response and homeland security, including the role of the National Guard. Generally, the dialogue supports an increased role in homeland security for the National Guard, differing only in details. The Governors agree with that general

direction, and encourage the continuation of the dialogue. Because of the uncertainty surrounding the final definition of the Guard's role in homeland security, a 405,000 force-structure may no longer be appropriate.

The National Guard has not been immune from post-Cold War force reductions. In fact the National Guard today is at the same force structure level as prior to World War II. With the support of the President, the Secretary of Defense, and the Secretaries of the Army and Air Force, we have been able to maintain an Army and Air National Guard that is capable of meeting our national security needs and of ensuring that the Governors have under their command the right mix and numbers of forces to meet the myriad emergency and domestic missions that are unique to the National Guard. The Governors are committed to the National Guard continuing to be the primary reserve force in our country. It should continue to play a critical role in peace and war.

The Army and Air Force are encouraged to commit to the full preparation of and maximum, practical utilization of the National Guard as a dual-missioned force for both domestic and outside the continental United States (OCONUS) peacetime and wartime missions. The Guard's effectiveness in responding to state and federal domestic emergencies is a direct result of its combat, combat support, and combat service support missioning, training, equipping, and deployment experience. The National Guard's strengths are the quality and combined military and civilian training of its people, its unique state and federal ties, its unique dual mission, and its cost-effectiveness and combat readiness. It is the national insurance policy for domestic and foreign emergencies.

## **6.6 Equal Opportunity in the National Guard**

The National Guard is composed of men and women of all races, colors, creeds, and religions from more than 3,600 communities in the states, territories, and the District of Columbia.

The National Guard Bureau has established equal opportunity in the Guard as one of its primary goals. It is attempting to ensure fair and equal access to all positions in the National Guard.

The Governors, as commanders-in-chief of the National Guard, fully support equal opportunity in all state programs and institutions under the Guard regardless of race, sex, or religion; endorse the National Guard Bureau's goal; and pledge full support in achieving equal opportunity in all aspects of the Guard.

*Time limited (effective Winter Meeting 2003-Winter Meeting 2005).  
Adopted Annual Meeting 1986; revised Annual Meeting 1990, Winter Meeting 1991,  
Annual Meeting 1992, Winter Meeting 1994, and Winter Meeting 1995; revised and  
reaffirmed Winter Meeting 1997; reaffirmed Winter Meeting 1999; revised Winter  
Meeting 2001 and Winter Meeting 2003 (formerly Policy B-5).*





### *Policy Position*

## **HR-10. Terrorism and Homeland Security Policy**

### **10.1 Preamble**

The terrorist attacks on September 11, 2001, reveal that the threat of catastrophic terrorism across our nation today is a real and complex phenomenon. Threats involving nuclear, biological, and chemical weapons and attacks on critical infrastructures, including water, fuel, communications, and computer systems, can strike at any time. As a result, strategic intergovernmental preparedness and interagency cooperation at all levels of government are essential ingredients to prevent loss of life and major property damage. Because these incidents start on the local level, it is imperative that planning and training for state and local response forces be included in any national strategy.

Governors have a critical interest in domestic terrorism because responding to the consequences of terrorist events is clearly within their authorized roles and responsibilities. Governors, with the support of the federal government, are responsible for ensuring the ability of state, territorial, and local authorities to deal with natural disasters and other types of major emergencies, including a terrorist incident.

### **10.2 Challenges for States and Territories**

There are many challenges for states and territories in managing the consequences of terrorism, including preparing people to cope with new and stressful challenges while handling information needs, managing consequences, preparedness and mitigation efforts, clarifying the role of the National Guard, and supporting public-private cooperation.

**10.2.1 Handling Information Needs.** Many of the operational, programmatic, and funding activities associated with terrorism consequence management preparedness are classified because of national security. Thus, the sharing of critical information is hampered. Although provisions exist for sharing information concerning ongoing actual events, dealing with preparedness activities is more problematic. Governors and other high-ranking state and territorial officials need to receive timely and critical intelligence information related to terrorist threats. Security clearances should be standardized and reciprocal between agencies and levels of government. There is also a need to receive federal security clearances more expeditiously. In addition, relevant nonclassified

information about terrorist threats needs to be disseminated to state and local authorities who are charged with providing immediate responses to these threats. Overall, state governments must be viewed as strong partners in the United States' national security efforts, particularly as related to terrorism. Encouraging liaisons with the FBI, the Bureau of Alcohol, Tobacco and Firearms, the Secret Service, and other national security agencies to be detailed to the appropriate state and territorial authority would greatly help in the dissemination and sharing of critical information in a timely fashion.

**10.2.2 Prevention, Detection, and Deterrence.** Governors recognize that in order to protect their states and territories from potential terrorist events, they must effectively integrate all sectors of state government that are affected by homeland security issues. Relevant sectors of state government are actively involved in prevention, detection, and deterrence as well as response and recovery efforts following terrorist acts. States' management of potential crises through prevention, detection, and deterrence is as essential as their response to terrorist acts. To prevent an attack, it is vital that the collection and analysis of critical information be shared across a broad spectrum of groups both in the public and private sectors. Governors play a vital role in ensuring the integration of federal, state, and local homeland security structures and involvement of the private sector in order to provide access to information that may prevent terrorist activity. Information collection and sharing is necessary to enhance the capability and capacity of first responder agencies.

**10.2.3 Managing Consequences.** Managing the short- and long-term consequences of terrorism is among the responsibilities of state and local government supplemented by the resources of the federal government, coordinated by the U.S. Department of Homeland Security (DHS). Issues related to activities such as initial response, the need to manage large numbers of potentially contaminated victims, evacuations, widespread need for security in communities following an event, and short- and long-term recovery are some of the many responsibilities incumbent on state and local elected officials.

In the aftermath of the September 11, 2001, attacks, states and territories have borne unprecedented costs to ensure that the nation's critical infrastructure and the public are protected. At the request of the President, Governors provided security for the nation's 425 commercial airports. Subsequently, they provided security for facilities, such as nuclear power plants, ports and border crossings, pharmaceutical labs, communications towers, and other critical infrastructure. The federal government and the private sector are responsible for securing most of these facilities, but Governors believe that whatever is needed for security and protecting lives must be accomplished. However, the use of the National Guard and state and local law enforcement in overtime status has been very costly to states. Therefore, the federal government should reimburse states for this protection, since it is originally its responsibility.

Furthermore, Governors believe that when the National Guard is performing domestic missions, it should be used in Title 32 USC status rather than Title 10 USC status. In Title 32 status, National Guardsmen can continue to train with their regular units, and in times of mobilization, these Guardsmen are available to deploy with their units. This is

not the case in Title 10 status, where they would not be available for continued training or deployment with their unit. Readiness may suffer when these troops cannot train in their combat specialties, and the unit suffers if it has to deploy without its full complement. Also, Title 32 status avoids any posse comitatus issues.

**10.2.4 Supporting Public-Private Cooperation.** Terrorism preparedness efforts should be inclusive of key private sector entities such as defining the appropriate roles and responsibilities for public and private health and medical communities. The role of the business community and the impact on the economic viability of a community when faced with recovery from a terrorist attack must be considered. Preparedness and recovery efforts should focus on ensuring that limited federal resources are effectively allocated across all geographic areas and coordinated with the Governors to achieve a truly viable and effective national capacity.

**10.2.5 Clarifying the Role of the National Guard.** The role of the National Guard in terrorism response activities is to support federal, state, territorial, and local response agencies with equipment, facilities, and personnel. The National Guard, historically a critical resource in emergencies, can be an effective force multiplier to civil authorities in responding to terrorism at the state, local, and federal levels. In the wake of the September 11, 2001, attacks, the National Guard has expanded its traditional role in homeland defense and security. National Guard activities include securing strategic facilities, such as airports, pharmaceutical labs, nuclear power plants, communications towers, and border crossings, and have been a cornerstone in protecting our citizens from domestic terrorism. The U.S. Department of Defense should reaffirm these activities as an integral part of the ongoing mission of the National Guard and ensure that they are provided the funding, training, and other resources necessary to fully meet the additional responsibilities inherent in today's homeland defense environment. Any assignment of responsibility should enhance the nation's terrorism consequence management capability and provide for the contingency of the National Guard being called to assist active and reserve components in dealing with a major military conflict.

### **10.3 Federal Responsibility**

The unique nature of terrorism coupled with national security implications requires the support and expertise of the federal government in working with state, territorial, and local government in developing capabilities. A clear national strategy developed through a partnership among federal agencies and key state, territorial, local, and private sector stakeholders is essential to drive operational and programmatic planning, training, and service delivery in combating terrorism.

Governors recognize the need to coordinate programs among federal agencies to address terrorism and appreciate and support the efforts of the Department of Homeland Security. There should be greater clarification of the currently fragmented structure of federal responsibilities and more cooperation among federal agencies to better enable states and territories to plan for terrorism responses.

The National Strategy for Homeland Security, signed by President Bush July 16, 2002, articulates a comprehensive strategy for the common defense of the nation that reinforces the historic role of Governors in providing for the citizens of their states and territories. Therefore, Governors urge appropriate funding and reimbursement to states and territories for providing security for the critical infrastructure, maximum coordination of program components, and coordinated service delivery within states, territories, and localities. The Governors urge that all federal homeland security funding, including funds earmarked for local jurisdictions, be distributed through the states and territories in order to enhance regional response capabilities within the states and territories and to advance the comprehensive homeland security strategy of each state and territory.

#### 10.4 Conclusion

The articulation of policy goals and the desires of local, state, territorial, and federal leaders should serve as the foundation for establishing any corresponding operational and programmatic work effort regarding terrorism. It is especially important that input from the nation's Governors continue to be solicited when updating the homeland security strategy. Any update and legislative and/or administrative policy concerning the strategy should be based on the following principles.

- Federal departments and agencies should work with state, territorial, and local governments to develop strategies, plans, and programs related to homeland security.
- Funding for all infrastructure protection and public health systems should be coordinated through the appropriate state and territorial agencies.
- Federal departments and agencies must coordinate with and through the states and territories when delivering federal assistance to first responders.
- Adequate resources must be provided to support any proposed security need that would require state and local participation.
- The National Guard is the primary reserve component of the United States Army and Air Force. It must remain "dual missioned" and must be properly trained and fully equipped and resourced by the federal government to perform both homeland security missions and traditional combat, combat support, and combat service support missions.

A well-developed national strategy and work plan, reflecting the desires and needs of local, state, territorial, and federal policy officials, should guide the development and approval of national programs and policies. Maximum resources must be combined with state, territorial, and local efforts to achieve a truly viable national capability to prepare and manage the consequences of terrorism.

Note: Many of the principles in this policy are similar to those in policy HR-25, Emergency Management.

*Time limited (effective Winter Meeting 2003-Winter Meeting 2005).*

*Adopted Winter Meeting 1999; revised Winter Meeting 2001, Winter Meeting 2002, and Winter Meeting 2003.*



---

---

**QUESTIONS AND ANSWERS SUBMITTED FOR THE  
RECORD**

MARCH 13, 2003

---

---



## QUESTIONS SUBMITTED BY MR. MEEHAN

Mr. MEEHAN. General Rees, the Report on the Impact of the Army Aviation Modernization Plan on the National Guard (dated 21 Jan 03) identifies an ARNG requirement of 783 utility aircraft (UH-60) through FY09 with only 687 aircraft projected to be in Army National Guard (ARNG) inventory at the end of that same fiscal year. What types of investment—both funding and equipment—is necessary to adequately address the projected shortage of 96 aircraft so that the Aeromedical Army National Guard units can continue to support their “full” mission requirements?

General REES. While the Army staff assesses lessons learned in recent combat operations and guidance from Office of Secretary of Defense and Army headquarters, the Army will delay further cascade of modern aircraft from the active component to the ARNG. When cascades are completed in accordance with the approved Aviation Modernization Plan, the ARNG will still be short 96 UH-60s. Ninety-six UH-60s provide the three aircraft needed to reach the doctrinal requirement of 15 for each of the 12 “warfight” ARNG Air Ambulance companies and the 15 aircraft needed to replace the legacy UH-1s in each of the four generating force ARNG Air Ambulance companies. The cost of 96 UH-60s depends on what year procurement would begin, how many are procured each year, and the specifics of the contract. A good estimate is one billion dollars, not including inflation considerations. Note that the estimated procurement cost does not include the communications equipment, aircraft survivability equipment, transportability equipment for deployments, extended range fuel systems, medical items mounted on the aircraft, and other items that directly support the aircraft.

Mr. MEEHAN. General Rees, due to a Department of the Army cap on UH-60 procurement—driven by funding constraints—the Army Aviation Modernization Plan eliminated four ARNG MEDEVAC companies, which incidentally is the same number as those units in the ARNG that still retain UH-1 Vietnam era helicopters. As I understand it, however three of these units are now on alert or have been activated to support the Global War on terrorism. Thus, given the potential homeland defense and security requirements—still under development/evaluation—and the current mobilizations what are your thoughts on: (1) first the need to retain these Aeromedical units; and (2) second, the need to take action to modernize and recapitalize the equipment of the four companies to ensure that they remain viable to address the existing and potentially new and expanded requirements on the horizon?

General REES. First, it is prudent to retain these four aeromedical units, because they can contribute in several roles. The companies continue to provide teams for aeromedical support to Army installations throughout the Continental United States (CONUS), while the active Army aeromedical units are deployed for combat operations. Specifically the ARNG aeromedical teams are supporting soldiers participating in CONUS-based training including the Army ranger camps (Mountain & Florida camps) and military families dependent on installation services. Additionally the companies can support state or federal authorities with responsive aeromedical capabilities to deal with a wide range of Homeland Defense situations from natural disasters to Weapons of Mass Destruction. If equipped with UH-60s the companies can deploy overseas in support of the full spectrum of military operations. Second, the Army needs to equip these units with modern aircraft to ensure long-term unit readiness and the capability to operate in combat theaters. The UH-1s are scheduled for retirement in one year, but may be extended for a few years due to the delay in cascade of UH-60s to the ARNG. However, extension of UH-1s is only a temporary solution. A modern aircraft, probably the UH-60 as the Army standard aeromedical aircraft, should replace each UH-1. As the requirement for scheduled rotation of deployed Army units expands to more military theaters, the requirement for UH-60 equipped aeromedical units also expands. Note that despite the versatility of these aeromedical units, it is not certain that Army headquarters will keep them in the force.

Mr. MEEHAN. I am concerned, as are other members of this committee, that the Army is funding—based on budgetary constraints—missions at the 80% level, add to this the fact that the current modernization plan states we will lose four ARNG

units (equivalent to providing the capability of approximately 48 aircraft when funded at 80%) and the requirements that the ARNG will be able to meet seem to drop exponentially. If a significant investment is not made in the immediate future, we could lose these four ARNG units that provide critical capabilities to support and defend our states and our nation. This is a critical time in our nation's history, we are engaged in the Global War on Terrorism, including a possible expansion of our efforts to Iraq, the administration's number one priority is to protect and defend our homeland, and the requirement to support emergency response missions in our states is not going away. As such, it seems imperative that we take action now to modernize and recapitalize the ARNG fleet, what do you see as the resulting impact on the ARNG ability to meet the warfighting, emerging homeland security and defense, and emergency response missions in the near and mid term?

General REES. The ARNG will suffer a major negative impact if the ARNG aeromedical fleet is not modernized and recapitalized. The four aeromedical units currently supporting CONUS Army installations can fill all three roles—the overseas warfight, homeland security and defense, and emergency response on the state level. Given the multiple demands for ARNG aeromedical capability, a decrease in the units will require longer and more frequent ARNG aeromedical deployments or a reduction in critical life-saving support. The four ARNG aeromedical companies should be equipped with UH-60s, at least at the 80% level, to ensure adequate aeromedical support for the Army and the nation.

### QUESTIONS SUBMITTED BY MS. SUSAN DAVIS

Ms. DAVIS. General Rees, my district includes a portion of the Southern Border. For a long period of time National Guard units were at border points of entry. I heard many frustrations about their lack of ability to participate in Border security functions such as inspections and detentions. Should we routinely place troops at the border to assist Border Patrol, Customs, and Immigration agents?

General REES. The Department of Defense and the National Guard can give assistance to federal agencies, such as the Department of Homeland Security. When discussing deploying U.S. troops to provide assistance to law enforcement agencies the issue of violations of the Posse Comitatus Act (PCA) are important. The PCA restricts use of Title 10 active duty military personnel. The statute also applies to the National Guard when activated in a Title 10 (Federal) status. The statute does not apply to National Guard personnel in a Title 32 (State) status. Over the last fourteen years, the National Guard Counterdrug Governor's State Plans program has provided military support (in Title 32 status) to state, local, and federal agencies operating at the nations borders. In a 13 February 2003 memorandum, the Deputy Secretary of Defense approved a plan to transfer these duties to the Department of Homeland Security. Specifically, the National Guard will no longer provide cargo and mail inspection augmentation at the borders, though will continue with its Surface Reconnaissance, Aerial Reconnaissance and Imagery/Mapping support to law enforcement agencies.

**FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT—DEPARTMENT OF DEFENSE EFFORTS TO ADDRESS THE CHEMICAL AND BIOLOGICAL THREAT**

---

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ARMED SERVICES,  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES  
SUBCOMMITTEE,

*Washington, DC, Wednesday, March 19, 2003.*

The panel met, pursuant to call, at 2 p.m. in room 2118, Rayburn House Office Building, Hon. Jim Saxton (chairman of the subcommittee) presiding.

**OPENING STATEMENT OF HON. JIM SAXTON, A REPRESENTATIVE FROM NEW JERSEY, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. SAXTON. The committee will come to order. Good afternoon.

Today, the Subcommittee on Terrorism, Unconventional Threats and Capabilities meets to receive testimony on Department of Defense (DOD) policy and programs for countering the threat of weapons of mass destruction (WMD).

This hearing cannot be more timely. War with Iraq is imminent, and our Armed Forces and those of our allies will fight under the threat of possible use of biological and chemicals weapons by our adversary. Terrorist groups have actively sought to obtain the capability for the use of chemical, biological, radiological or even nuclear weapons and would pose the use of such weapons to achieve their objectives.

Weapons of mass destruction—nuclear, biological and chemical—in the possession of hostile states and terrorists represents one of the greatest security challenges facing the United States. In meeting this challenge, the Department of Defense plays major roles, both with respect to the capability of our Armed Forces and the support the Department provides to homeland defense.

The purpose of today's hearing is to gain an understanding of that role and the Department's organization, policy and programs for countering the potential threat of weapons of mass destruction and for ensuring the capabilities of our armed forces to fight on a battlefield under the threat of the use of such weapons.

To address these issues, we have our witnesses today:

The Honorable Dale Klein, Assistant to the Secretary of Defense, Nuclear and Chemical and Biological Programs; Dr. Stephen Younger, Director of DTRA, the Defense Threat Reduction Agency; Dr. Tony J. Tether, Director of DARPA, the Defense Advanced Research Projects Agency; Brigadier General Stephen Goldfein, United States Air Force Director of Joint Requirements for Chemi-



cal, Biological, Radiological and Nuclear Defense, the Joint Staff; and, finally, Brigadier General Stephen Reeves, United States Army, Joint Program Executive Officer, Chemical-Biological Defense Program.

Gentlemen, we welcome you and look forward to your testimony.

Before you proceed, I would like to recognize my friend and partner, Marty Meehan, for any statement that he might choose to make Marty, go ahead. The floor is yours.

[The prepared statement of Mr. Saxton can be found in the Appendix on page 131.]

**STATEMENT OF HON. MARTY MEEHAN, A REPRESENTATIVE FROM MASSACHUSETTS, RANKING MEMBER, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. MEEHAN. Thank you, Mr. Chairman; and let me thank you as well for scheduling this hearing and let me join you in welcoming the members of this panel.

Gentlemen, thank you very much for being with us this afternoon.

Mr. Chairman, like you, I believe the issue before us today is of utmost importance. No other effort should receive more attention than that devoted to countering the threat of weapons of mass destruction. No less than 25 nations currently possess weapons of mass destruction, and the real threat exists for these instruments of destruction to fall into the hands of terrorists.

As we will hear today from our panelists, countering the weapons of mass destruction threat falls to more than just simple investments in technology and development. Indeed, countering the threat requires a comprehensive and all-encompassing approach, one involving both technology development and nonproliferation initiatives. Securing diplomatic agreements, arms control measures and other threat reduction efforts often hold as much if not more promise as a pursuit of technology development.

In truth, a coordinated approach tempers the technological challenge facing our Nation's scientists. It is the threat reduction part of DTRA.

Mr. Chairman, I thank you for scheduling this hearing; and I look forward to hearing and questioning our panelists.

[The prepared statement of Mr. Meehan can be found in the Appendix on page 134.]

Mr. SAXTON. Thank the gentleman for his statement.

As I indicated before, our first witness is Dr. Dale Klein, Assistant Secretary of Defense for Nuclear and Chemical and Biological Programs.

Dr. Klein, the floor is yours, sir.

**STATEMENT OF DR. DALE KLEIN, ASSISTANT TO THE SECRETARY OF DEFENSE, NUCLEAR AND CHEMICAL AND BIOLOGICAL DEFENSE**

Dr. KLEIN. Thank you, Mr. Chairman, ranking member and distinguished members of the committee. It is a pleasure for us to be here today, for me to appear with my fellow panelists and describe

our programs to protect the men and women in uniform as they carry out their tasks.

At the direct request of the committee, we have concentrated today on the chemical and biological defense programs. Each panelist is prepared to give a small, brief opening comment. We have submitted extended comments for the record for your staff to consider. With your permission, we will take just a moment to focus on some key issues, and then we will answer your questions. In the event that we are unable to answer your questions fully, either due to security concerns or other reasons, we will respond to your questions in detail promptly after this hearing.

I would like to make two points before we begin. The first one is that we have no chemical weapons in the United States other than our obsolete stockpile for which we are dismantling. All of these weapons are in the United States. They are being dismantled by international inspection, and they follow the rules of the treaty and by law. All the chemical weapons, the old obsolete weapons that we have, are in the continental United States.

The other point is that we have no biological weapons. The Department of Defense ceased their offensive biological weapons program over 30 years ago.

Second point is that, as we are all aware, we have thousands of U.S. Troops and coalition forces poised to take action if called upon by the Commander-in-Chief. Each of the panel members before us have the thoughts and prayers for those individuals that will be likely called into action to accomplish a very difficult task.

Specifically, when you look at the panel members before us, Dr. Younger has over 100 members of his team, experts in the field, forward deployed to minimize the consequences of the Iraqi use of weapons of mass destruction.

Items that have been procured under the leadership of Dr. Reeves are either hanging on the belt or flowing in the veins of the warfighters that are forward deployed.

Under the leadership of Dr. Tether, we have the technology advances that will enable us to have an edge over our foes in this potential conflict or the next.

In addition, General Goldfein has a vital role in the Joint Staff in validating our operational military requirements in the area of nuclear, chemical, biological defense areas to ensure that the needs of the warfighter are met.

In Operation Desert Storm, my wife was deployed in southwestern Asia as a medical evacuation unit member along with other Air Force reservists. I have learned firsthand of the status of the chemical and biological defense programs at that point in time.

Since the last year and few months, I have learned of the programs that we have in the Department of Defense currently; and I can assure you that our warfighters are much better prepared to fight and win in a weapons of mass destruction environment than they were in 1991. If the leadership in Iraq miscalculates and uses weapons of mass destruction, our warfighters are prepared to continue on their mission and enforce the U.N. Resolutions and assure us that weapons of mass destruction will not be in Iraq under a future regime.

We have asked General Reeves to bring a few examples of some of the equipment that our troops are provided in the southwestern Asia region, and later on he will go through and give some examples and talk about those in a little bit more detail.

I should point out, even though General Reeves has on an Army uniform, he represents all of the services in all of the Department of Defense and, in addition, provides some technology and equipment to other agencies outside of the Department of Defense.

With your permission, I would ask that our written testimony be submitted for the record and that we then have brief opening comments by other panelists; and then we will respond to your questions.

Mr. SAXTON. Dr. Klein, thank you; and without objection each opening statement will be placed in the record in its entirety.

[The prepared statement of Dr. Klein can be found in the Appendix on page 137.]

Mr. SAXTON. We will turn now, I guess, to Dr. Younger.

#### **STATEMENT OF DR. STEPHEN YOUNGER, DIRECTOR, DEFENSE THREAT REDUCTION AGENCY**

Dr. YOUNGER. Mr. Chairman and members of the committee, it is an honor for me to be here this afternoon to represent the work of the fine men and women of the Defense Threat Reduction Agency. I would like to make a few comments to begin with.

Starting with the job of the Defense Threat Reduction Agency, it is simple, and it is vital, and that is to make the world safer by reducing the threat of weapons of mass destruction. We employ a comprehensive approach involving five tools:

First of all, arms control. We go to other countries and verify that they are abiding by their conventional and nuclear weapons treaties.

Second, cooperative threat reduction. If we find something, we work with the other country to destroy it in an effective manner.

Third, technology development, also known as an uncooperative threat reduction program. That is, we develop new weapons to destroy WMD in place before they are used against our forces.

Fourth, chemical and biological defense. If something gets through, then protect our troops against it. We expect to assume new leadership duties in science and technology associated with chemical and biological defense.

And, fifth, combat support. We are a combat support agency. We exist to support the commands, the services and the National Guard. We help with planning. We do targeting. We keep track of our Nation's nuclear arsenal, and we perform vulnerability assessments in the United States and at installations around the world. We use the best technology from government, industry and universities to create new products of direct utility to the warfighter and to the Department of Homeland Security. In that sense, we are a can-do/go-to agency covering the entire spectrum of defense against weapons of mass destruction.

Some of our recent successes include three new classes of weapons for the warfighter. We delivered a thermobaric weapon in less than 30 days, we delivered a new class of agent defeat weapons in less than 6 months, we delivered thermobaric weapons on the

Hellfire missile in 13 months, and I am pleased to say that they are in the operational theater at this time.

We have deployed a new system to protect bases against nuclear and radiological weapons. We have developed a test bed for advanced biodefense in American urban areas. I am pleased to say that a set of play books that we developed in response to weapons of mass destruction incidents in American cities is being used as the foundation of our national response plan for those catastrophic events.

We have a 24/7 operations center to support Northern Command and other components of the Department of Defense; and, again, we provide vulnerability assessments for all of the buildings of the Capitol, many other buildings in Washington and military installations around the world.

Weapons of mass destruction do indeed represent one of the most serious national security threats to the United States, and the Defense Threat Reduction Agency is reducing that threat. Thank you.

Mr. SAXTON. Thank you very much for a very nice, concise statement.

[The prepared statement of Mr. Younger can be found in the Appendix on page 152.]

Mr. SAXTON. Dr. Tether.

#### **STATEMENT OF DR. ANTHONY TETHER, DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECT AGENCY**

Dr. TETHER. Thank you very much, Mr. Chairman, for having me today. I would like to have my written testimony entered into the record.

We have what we feel is a good framework for looking at the problem in five stages of time: from before the attack, during the attack, minutes to hours after, hours to days after and then the clean-up phase. My written testimony goes through all of those stages and gives examples of programs that we have ongoing, and so I won't dwell on those.

However, we really do feel that the greatest strengths of our fiscal year 2004 program is the fact that we do cover the span from trying to prevent the attack from occurring in the first place all the way to if we have to clean up after the attack. If you recall with the Hart building, that was a major chore in doing that.

When somebody says they have a strength, there is always a tempting question to say, well, if you have a strength, you must have a weakness someplace. If I were to say that we had a weakness—and I don't consider it necessarily a weakness that, especially in the drug part, the vaccine part that we work on, it is, how do we get it through the FDA process? That becomes a problem. How do we transition this out to industry to have industry and the pharmaceutical companies actually make the drugs?

With that in mind, the DARPA program has always been focused on how to overcome that shortcoming. For example, one of our major programs is our unconventional pathogen program, is trying to create one drug which would attack many bugs. We have been successful in that. Our reasoning behind it was to try to find something in each bug that was common that we could then create a drug which would attack it. Our hope was to have one of those



bugs be a commercial bug, one that we all just get as a matter of course, in which case we could get the pharmaceutical companies to be interested in taking that drug through the process and at the end of the day not only have a drug for a commercial disease but also have a drug for the more exotic diseases that we all worry about.

The last thing is, as you know, DARPA is an unusual place; and we are sort of independent and different from every place else. One good question is, how do you coordinate with everybody else? How do you know that what you are doing is going to be transitioned into the forces?

We do that a couple of ways. We have meetings. It is a contact sport for transitioning. It really becomes people knowing what other people are doing. So—like Steve and I have had meetings at his place. He has been to our place.

In the fiscal year 2004 budget, there is money set aside in the Army part of the budget for specifically transitioning technologies; and, in fact, money is there for specifically transitioning DARPA technologies, which is really a great help. That means, as we develop something, there is money already in place to be able to take our technologies and transition it; and that seems to be working out. The fiscal year 2004 amounts were higher than they were in years past. But they are adequate.

With that, I will just end my testimony. Thank you very much.

Mr. SAXTON. Thank you very much.

[The prepared statement of Dr. Tether can be found in the Appendix on page 144.]

Mr. SAXTON. We will now move to Brigadier General Stephen Goldfein.

**STATEMENT OF BRIG. GEN. STEPHEN GOLDFEIN, USAF, DIRECTOR, JOINT REQUIREMENTS OFFICE, CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR DEFENSE (J-8), JOINT STAFF**

General GOLDFEIN. Mr. Chairman, gentlemen, good afternoon.

Last year, the Chairman of the Joint Chiefs directed that—

Mr. SAXTON. I am sorry. Could you pull that microphone toward you a little bit?

General GOLDFEIN. Last year, the Chairman of the Joint Chiefs of Staff directed the formation of a Joint Requirements Office for Chemical, Biological, Radiological and Nuclear Defense. The intent was to represent the warfighter, to develop concepts and ensuing architecture, to help to identify and prioritize capabilities for our defense. I am honored to be the representative as a director of this organization, and I look forward to the discussion.

Thank you.

Mr. SAXTON. Thank you, sir.

[The prepared statement of General Goldfein can be found in the Appendix on page 159.]

Mr. SAXTON. Brigadier General Stephen Reeves.



# STATEMENT OF BRIG. GEN. STEPHEN REEVES, USA, JOINT PROGRAM EXECUTIVE OFFICER, CHEMICAL AND BIOLOGICAL DEFENSE PROGRAM

General REEVES. Mr. Chairman, members of the committee, my name is Steve Reeves. I am the program executive director for chem/biodefense; and we are located in Falls church, Virginia.

Today, what I would like to do is show you the results of the work that the joint services have done collectively in identifying new requirements and the joint service acquisition community has done in providing the men and women that are in the Gulf today with the best equipment in the world.

I would like, with your permission, sir, to bring up and begin with the individual protective mask and allow the members to individually see that, if that is all right.

Mr. SAXTON. Sure.

General REEVES. This is the new protective mask. We did not have this protective mask during the Desert Storm period. It is a substantial improvement over the previous mask. As you can see, it has an external cannister. It protects against all known and suspected biological and chemical agents that are in the Gulf today. It has improved vision. It provides ballistic protection, in other words, protects against shrapnel and shards and other stray pieces of metal. It provides inherent to it an ability to hydrate. In other words, you can hook a hose up to a canteen to make sure you have plenty of water.

More importantly, the mask is fundamentally different in its design because it has an internal—what we call a face blank. But it is a silicone seal that fits around the face. It provides a better seal. It is more comfortable. The air on the inside of the mask is specifically designed to recirculate over the lens so that you don't have any fog on the lens, and psychologically it makes you feel less claustrophobic.

We ensure that each one of our warfighters have a proper fit with this mask using a system called the Protective Assessment System. Each mask is literally individually fitted to the warfighter, and we ensure that that seal is appropriate for that person's face.

Mr. SAXTON. General, the round cannister on the front of the mask, Jean Reed tells me, is a biofilter.

General REEVES. It is both a chem and biofilter.

Mr. SAXTON. How long does that last?

General REEVES. Once contaminated, we recommend that it be changed within 24 hours. Otherwise, it is good up to a year.

Mr. SAXTON. Would you demonstrate for the committee members how you change that cannister?

General REEVES. You bet.

The problem with the older mask was that the filters were embedded along the sides of the mask, very difficult to change; and you had to take the mask off to change it. With this mask, the filter simply unscrews; it self seals. There is a seal in here so you can change it in a contaminated environment, take a new filter out, and it simply screws back on.

Mr. SAXTON. There is a similar port on the other side of the mask, isn't there?

General REEVES. That is correct.

One of the things we designed this mask specifically for was the various missions of all of our services. If you are like me and you are left-handed and you are trying to fire a weapon, then you want to make sure the filter is on the opposite side of where you would normally have it so that you could get your weapon up.

Along with the mask, we have a new generation of protective overgarment called the JSLIST or Joint Service Lightweight Integrated Suit Technology. What the Commander is holding up right now is the JSLIST suit. It has an integrated hood that comes over the back of the head so when you put the mask on you have a completely encapsulated seal. The suit is lighter. It is more durable. It lasts 120 days out of the bag or 45 days while wearing. It can be laundered up to six times and provides protection, again, against all known or suspected biological or chemical agents.

Mr. Chairman, I have personally worn this suit and this mask in a live chemical agent environment in August in 90 degrees heat and 90 degrees humidity. And during the six hours that I wore that, was it uncomfortable? You bet. Was it survivable? Absolutely. There are 70,000 other soldiers, sailors, airmen and Marines who have been through that same training; and we have never had a single accident. So we are confident this equipment works in the appropriate environments.

Mr. SAXTON. This equipment is deployed with the forces that are currently preparing to go into Iraq?

General REEVES. That is correct. Our ground forces each have two of these suits available to them.

Along with that, there is also some individual equipment. This includes skin decontamination equipment which each of our warfighters carries. This equipment is actually a pad. It is used for hasty decontamination in the event you are contaminated. It consists of an activated powder. It has been approved by the Federal Drug Administration (FDA) for use on the skin.

In the event of the worst-case situation where you actually are contaminated with a nerve agent, each of our warfighters carries three autoinjectors which are taken out. As you see it here, you literally stick it into your thigh and the needle comes out and injects with one of two things, either atrophine or 2-PAM chloride. And you use one of each.

As the stocks of these are expiring, we are replacing them again with another FDA injector. This time we put both drugs in the same injector, so you have a single injector, again a product of the chem/biodefense program.

In supporting selected units and as the need arises, we have a lotion that goes with the suit. So if you are wearing your suit for an extended period of time, if you get chafing around the neck from wearing it or in other areas where you might have a rub, this is a lotion that provides barrier protection against biological agents, again FDA approved, and provides a seal on that suit. It is called SERPACWA—and this, Mr. Chairman, is a name that only the DOD and FDA could come up together with—Skin Exposure Reduction Paste Against Chemical Warfare Agents.

The last piece of individual equipment I would like to talk about is the pocket Radiation, Detection, Indication and Computation (RADIAC) meter. This gives both instantaneous dose reading—in

other words, when you move into a contaminated area, what is the immediate dosage you are receiving, but it also keeps a collective dose. Of course, with radiation—we are concerned with exposure over time with radiation.

Finally, in terms of smaller equipment, we have what we refer to as a hand-held assay. These are assays that are used for detecting biological agents. It was a kit similar to this that detected the anthrax in Senator Daschle's office.

This looks and acts very much like a home pregnancy kit. You take a suspected biological sample and put it in a small well. One line tells you you have done the test correctly; and if you see the second line, then you know you have a problem.

These test kits are configured in packages of eight, and we specifically configure them based on whatever the biological threat is in the area that our forces are operating.

Mr. SAXTON. That is pretty good progress. Didn't we have to take a swatch of material back to the lab previously to have it tested?

General REEVES. During the Gulf War, we virtually had no biological detection capability whatsoever; and we have made huge progress in the biological detection areas.

As we have also learned our lessons from that Gulf War, we have also improved our chemical detection. We have a new chemical detector called the Automatic Chemical Agent Detector Alarm. Again, we have procured over 20,000 of these and deployed them with our joint forces. This alarm was specifically and extensively tested as a result of our very unfortunate false alarm experiences with the old maximum allowance (MA) alarms. We tested it against over 80 potential battlefield interferences to ensure that when the alarm goes off we have a positive.

Now I won't kid you. There is still going to be a one to two percent false positive rate. That is just simply the nature between chemistry and physics. But this has substantially reduced the false positive rates we have had in the past.

We have also specifically designed it so that it would simultaneously detect both nerve and blister agents. We designed it to use a common battery instead of a unique battery. We designed it so that you can get either a visual or audible signal or both, because there may be situations where you simply don't want to have the audible signal.

Along with that, we have a second detector that is used for close-in detection, specifically to ensure you have decontaminated equipment on the ground, called the Improved Chemical Agent Monitor, same principles, same improvements in terms of interference.

Mr. SAXTON. I saw a television story that we have chickens and pigeons in the theater; is that right?

General REEVES. I believe, frankly, Mr. Chairman, that all of the chickens have died. I am sure this is well intended, and I am sure that the thought at the time was that this would act something like the canary in the mine. The problem with the analogy is that the canary in the mine was trying to detect methane and the miners would wait until the canary stopped singing. If you waited until the canary was dead, you were probably going to be dead as well. We suggested the chickens probably aren't such a good idea. The pigeons pretty much fall in the same category because, at best,

they have an equivalent sensitivity to the person; and obviously what you want is the earliest possible warning.

The automatic chemical agent detector is something like a thousand times more sensitive than a human to chemical agents in the air.

All of that said, let me suggest that that is a management answer. If you are a leader and that gives your soldiers or Marines more confidence, as long as they have got their other detectors with them, I would suggest that may not be all that bad.

Finally, Mr. Chairman, we do have a recently licensed FDA product in theater, although at the moment there appears to be no reason that we would have to issue it. It is called Pyridostigmine Bromide, frequently abbreviated PB. These are pills that you take specifically if you believe there is a threat of the nerve agent soman.

This is the first drug that has been licensed under what the FDA refers to as the animal rule. One of the improvements in our medical area over the last year has been that, by using animal surrogates, we can now license certain products that we couldn't license before because we couldn't ethically prove their effectiveness in humans; and now, by using animals, we can do that. This is a pretreatment.

Again, there is no intention at this point to issue it, but it is there if needed.

Mr. SAXTON. Tell us again what that is—I guess you would call it a prophylaxis.

General REEVES. This is a prophylaxis against soman.

Mr. SAXTON. Dr. Klein mentioned in his opening statement or somebody did—I think it was Dr. Klein mentioned that our troops have preventive equipment in or materials in their veins or hung on their belts. Is what he was referring to?

General REEVES. These are the kinds of things in terms of the atrophine injectors, in terms of the nerve agents, the vaccines.

I am also responsible for medical products; and so the anthrax vaccine, smallpox vaccine, the two primary threats we see in the area were also provided to our warfighters.

Mr. Chairman, let me simply conclude by thanking the members of the committee and the Congress for their continued support of this program. That support has resulted in over 19 new systems to our ground forces and another 3 systems that are exclusive to our Naval forces and significantly improved our abilities since the Desert Storm period.

That concludes my testimony.

Mr. SAXTON. Thank you very much, General.

[The prepared statement of General Reeves can be found in the Appendix on page 157.]

Mr. SAXTON. The use of weapons of mass destruction is obviously a topic that causes everyone who is here and everyone who is at the table and in the chairs behind you a great deal of concern for all the obvious reasons. Each of the threats that we discussed is different. That is also fairly obvious. The threat aside from a nuclear device and aside from perhaps a dirty bomb device, so-called, the threat posed by biological weapons that would be used either on the battlefield or by terrorists has long caused me a great deal of concern; and I am wondering what is—what do you see, Dr.



Klein, as the best answer or the best way to combat that threat that we have available to us today?

Second, where do you see us going down the road? Are there some technologies that are showing promise or are we still where we were a couple of years ago?

Dr. KLEIN. Mr. Chairman, as you probably know, there have been tremendous advances in the molecular biology area. That is the good news. From the time that the scientists discover in the laboratory till the time that it is implemented and licensed sometimes takes some time. But for the warfighter in the field, what we have done for those individuals on the biological threats, we have vaccinated those individuals with what we think is most likely, that is anthrax and smallpox.

For what we are seeing in the future, the trend is to look at what happens at the cellular level so we can treat the toxins at the cell level so that we don't have to invent a vaccine and antibiotic for every situation. With the advances in DNA splicing, people can take something that is currently not a threat, make a slight modification, and then it can be a threat. Someone can alter an anthrax strain and cause our vaccine to be ineffective.

I think where we want to go long term is we would like to be able to treat at the cell level. We would like to have one-shot-does-all.

Obviously, we put a lot of money in cancer research, and we haven't gotten there, but we have a lot of bright people working on it. So I am optimistic in the future.

Mr. SAXTON. The notion of one-shot-does-all seems to me to be a critical kind of a notion inasmuch as there are so many strains of viruses and poisons, bugs, if you will, that can be used—that can be weaponized. Would you agree with that?

Dr. KLEIN. Absolutely. That is why it makes it difficult to have one shot for all. If we were to do that, someone would make a modification; and it would probably be ineffective. We need to go down to the root cause and understand at the cell level.

Mr. SAXTON. May I just turn to Dr. Tether on the same question. You know of my interest in this subject because we have talked about it over the years, and we are both aware of a project that is ongoing at George Mason University kind of along these lines. Could you give us an update on that project and how you see that going?

Dr. TETHER. You know, on the specific project, I don't think I can. But I will put that into the record for you.

On the one drug meets all, we obviously are working very hard on that; and, basically, at the cell level or at the DNA level is really where we are at.

It turns out that on the bugs of interests, if you were to look at their DNA, you find they have a higher concentration of the A and T part of DNA than you would find in humans. What we are doing is finding a drug that will attack that part of the DNA. If we attack that part of the DNA, we destroy the bug and also, because it is not normally in humans, where we will have a drug that won't attack a human.

If they try to mutate the drug—this is the part of DNA that might be called inert or the part of the DNA that is not doing the



harm but is needed to be there. If they try to mutate the bug, that part of the DNA will still have to exist in order for DNA to be viable. And they can mutate it all they want as long as we are still attacking it. That is what the research area is about.

Unfortunately, I don't know exactly what the George Mason current state of the art is.

Mr. SAXTON. We ought to look at that and maybe in a separate forum. Thank you very much.

Mr. Meehan.

Mr. MEEHAN. Thank you, Mr. Chairman.

General Reeves, the improvements that have obviously been made since the Gulf War seem to be significant. What is your assessment of the improvements and what else do we have on the drawing board in terms of improvements and what we give our ground troops? Is there anything else that is in the works that we could help facilitate?

General REEVES. Absolutely. We have structured the program in our budget request to recognize the needs to balance our program. When the Congress first recognized that we needed to focus our efforts in chem/biodefense after the Gulf War, we went after the high-priority issues. In my view, it is now time to bring balance to the program; and I believe our budget is doing that.

The budget has recognized the need to pursue greater advancements in biodetection technologies so we can get closer to detect war capability, to advance our standoff biodetection technology requirements. It has, second, recognized the need to address installation force protection; and we are doing that in our budget request. Finally, we need to address some areas that, frankly, were a lower priority initially but are certainly important to us; and that is the areas of decontamination and collective protection.

Mr. MEEHAN. Dr. Klein, the Joint Services Chemical and Biological Defense Program serves to ensure the protection of our forces; and we discussed some of the technologies to detect chemical and biological agents. How would the program potentially support our police and fire fighters and medical personnel if there was an attack in the United States, a chemical or biological attack; and what can we do to ensure that we get these technologies to our first responders? What do we need to be doing?

Dr. KLEIN. That is an area we are all very active in and I am sure Congress has been active in looking at that as well in terms of how do we help the Department of Homeland Security as they stand up and carry out their task.

What we really want to see happen is we do not want to see the wheel reinvented. There are a lot of technologies that have been developed through the Department of Defense that does have what we call dual-use application in the civilian sector. We are working very hard to make sure that information gets passed to the right people.

For example, Dr. Younger, through DTRA, is helping train a lot of the civil support teams so we work and we get those individuals trained with the current technologies.

As you know, the Department of Defense has a new individual now, Paul McHale, the Assistant Secretary for Homeland Defense. We are all working very hard to bring the civil section up to the

capabilities of what we know in the Department because it is a mutual benefit.

For example, we are charged, those of us here at the table, with defending our DOD facilities and people. But if there is an attack at a military installation, it is not likely to stop at the boundary. So we are working with a lot of communities on stand-off detection systems, Camp Lejeune being one. So we are working very hard on technology transfer.

Mr. MEEHAN. It seems to me that our ability to develop dual-use and also to get it to our first responders represents one of the biggest challenges that we have.

It is just amazing to see the advancements in terms of equipment and suits that have been made over the last few years, but when I look at police and fire departments and their uniforms that were developed in the 1940's and 1950's, I worry about the preparedness of those who are in the front lines here in the United States.

Dr. KLEIN. We are working very hard to help homeland security meet their mission. I think a lot of people, as you are aware of that, are working hard to see that happen.

Mr. MEEHAN. I am impressed to see the application of that to police, fire and medical personnel.

Dr. TETHER, the Defense Advanced Research Projects Agency's (DARPA) biological warfare defense program focuses on technologies that provide new approaches to the defense of the human body against any disease; and you have talked about some of them. The DARPA programs include the ability to block the entry of a disease-producing agent and medical diagnostic senses and decontamination. What are some of the promising technologies being pursued by DARPA for fiscal 2004, and how does the budget impact our capabilities for defense against biological warfare and biological terrorism for homeland defense and the Department of Homeland Security?

Dr. TETHER. One of the major efforts we have is on a process—an effort to basically try to take anthrax off the table. It is a program that—in fact, you all helped us along on getting the money for that; and that is moving along. It is roughly a 36-month program. We are getting close to about a third of the way through. What we are doing there is we are basically applying the same techniques that we had before on trying to find ways to look at anthrax and go to the fundamental part of the molecule and attack it.

We have six efforts ongoing. They are all proceeding. Unfortunately, I wish I could say they were ready to be used right now, but so far all of them are very promising.

The results that are coming out are all good at this particular stage. The resources that we need to pursue the program are adequate. I don't see any current need.

Of course, there could always be a surprise. The issue with it is, after we do this, how do we go the next step to get it to be useful for humans? The animal control thing for the FDA is very helpful. We will get to the point where we will be able to prove in animals that anthrax can either be a vaccine for anthrax, a therapeutic for anthrax, and then it will be able to be used on humans. So progress is very good.

Mr. MEEHAN. Thank you, Mr. Chairman.

Mr. SAXTON. Thank you.

The gentleman from Minnesota, Mr. Kline.

Mr. KLINE. Thank you, Mr. Chairman; and thank you very much, gentlemen, for being here today.

I can't tell you how excited I am to see the improvements. When last I had a chance to train some ten years ago, it wasn't nearly as good. So I applaud it. It is tremendous and long overdue.

I gather from your testimony, General Reeves, that you—I believe you stated absolutely and clearly that this gear, if worn by a warfighter over in the theater in and around Iraq, would prevent casualties from any known chemical or biological agent in that theater; is that correct?

General REEVES. That is absolutely correct.

Mr. KLINE. I am sure you have heard a great deal of speculation to the contrary, in fact, from some of my colleagues in the House, that equipment simply wasn't up to par; and I wanted to get it in the record that it absolutely was.

Following along the same lines, I believe you said that every warfighter in the theater has got two sets of these suits; and I want to see if I can make that clear to my old Marine Corps way of thinking. When you say warfighter, to me that means every man and woman who is on the ground in the theater, whether you are combat service or combat support or in a combat unit; is that correct?

General REEVES. That is absolutely correct. Just so—since you do have a Marine background, the Marines refer to their suits as Saratoga suits; and some of their packages are marked as Saratoga. So if you don't see Joint Service Lightweight Integrated Suit Technology (JSLIST) on the outside of it, it doesn't mean that it is different, it just means it has a different name.

Mr. KLINE. Outstanding. Thank you very much. And thanks for the great work.

Shifting just a minute if I could to Dr. Tether, you are the latest in a long line of very, very happy folks who have had that position as director of DARPA; and I am sure you are pleased to be there. I never met a director of DARPA who wasn't just elated at the fabulous opportunities that are there and the marvelous breakthroughs that DARPA has been responsible for over the years.

In previous administrations—I am talking about the administration of the director of DARPA, not necessarily a Presidential administration—there has been a focus of effort, for example, under Dr. Reese, perhaps it was simulation and modeling, what we now call the Internet and so forth. Can you give us some sense of the level of effort in this particular area that DARPA's got going now—half, third, most? By this area, I mean chem/biodefense.

Dr. TETHER. There is several parts to that chem/biodefense. One is the development of drugs to be able to either prevent you from having a disease or to carry if you have the disease. In that part of it, I would say it is on the order of five percent of the DARPA budget.

Now there is whole another part, and this is the part of detectors. One of the major problems that we have—first of all, we would like to try to prevent the threat from getting to the United

States in the first place; and we have efforts ongoing in that area. But one of the major issues is that—detecting the threat when it occurs and detecting it with sensors that don't have a large false alarm rate or a large false positive rate. That is a problem if you deploy in this building or wherever. It wouldn't take too many false alarms for people to just ignore it.

So we have another probably five percent of the DARPA budget working in the sensor technology, either developing smaller ultraviolet diodes, which could then be used to both detect the drugs and also to disinfect, and so forth and so on.

So I would say probably a total of ten percent of the DARPA budget is going to the general category of WMD, including both the drugs and also the detectors to detect that it happened so somebody would know to use the drug.

Mr. KLINE. I guess I am a little surprised that it is that low, frankly, considering the nature of the threat and certainly our heightened concerns about it today. And you are talking about percent of budget. Is that a pretty good measure level of effort?

Dr. TETHER. Not really. That is in the order of \$300 million, which is a lot of money in this type of research. If I were to talk to you about satellites and what our space business was, I mean \$300 million is barely an entry. For this area, \$300 million a year and the type of research we are doing is a lot of effort. It is a lot of people.

What we are buying is trying to reach out and find bright people with ideas that are different than one might go to National Institute of Health (NIH) with, and most of the people that we fund are people who typically are not funded by NIH because they have an idea with no data. It is those people that we reach out for because we take those people with an idea and we basically try to get the data to prove whether or not their idea is worthwhile, and then other organizations do take it over from that point on.

So \$300 million a year, from a number of people working on the problem, is a large number.

Mr. KLINE. So quite a bit more level of effort than the ten percent of the budget?

Dr. TETHER. Absolutely right. I probably—ten percent is really—it is almost the number of people you have working on the problem. In this area, \$300 million is probably equivalent to maybe two or three times that amount if I were building an airplane.

Mr. KLINE. I see my time has expired. Thank you very much. I yield back.

Mr. SAXTON. John, I had a retired Marine and an Air Force officer working for me—actually, the Air Force officer was a fellow in the last term. We were at one of our eight o'clock briefings, and somebody grumbled that we were starting too early and some were coming in too slow. And the Air Force officer said, well, if this was the Air Force, sir, by now we would be eating lunch. And the Marine looked up and said, if it were the Marine Corps, we would be taking in the afternoon paper.

Who is next? Mr. LoBiondo.

Mr. LOBIONDO. Thank you, Mr. Chairman.

One of my other responsibilities is chairing the Subcommittee on Coast Guard in the full Transportation Committee. We have been



struggling with the prospect of weapons of mass destruction somehow being delivered through our ports or our maritime facilities, and I am concerned about that.

We have talked a lot of what the Coast Guard is doing. For anyone on the panel, can you tell me if there are any interagency efforts that you are aware of participating to try to discourage this threat or deal with this threat or anything along these lines at all?

Dr. KLEIN. Mr. Congressman, let me talk a little bit about that in general on the nuclear side. We have a very active program—and I will let Dr. Younger talk a little bit more on it—on picking up radioactive materials. We have had—we have four test sites. Two of them are related on water areas, both at Kings Bay and at Camp Lejeune. So we do have some programs working interagency in terms of getting radioactive material, and I will let Dr. Younger talk about those.

Mr. LOBIONDO. Are you working with any other agencies in deployment of that technology?

Dr. KLEIN. We are working with the Department of Energy, Department of Justice and others.

Dr. YOUNGER. We are working with the Coast Guard to train them on the use of nuclear detectors. We have exercised with them.

As Dr. Klein indicated, we are working with the Department of Energy, Department of Transportation; and, more importantly, we are prototyping advanced systems for detecting nuclear materials that may enter a port via waterways. We have several technology programs under development for chemical and biological weapons as well. Ultimately, we will plan a system that will integrate all three—nuclear, chemical and biological.

Mr. LOBIONDO. Dr. Younger, I don't know how much of that may be classified, but I would like to explore with you separately whether we can do something with a Coast Guard hearing and if we need to be in closed session so we can integrate the Coast Guard Subcommittee on just what you are doing. Because this is an area that is a great deal of interest.

Dr. YOUNGER. We would be happy to help.

General GOLDFEIN. In our newly formed Joint Requirements Office, we have a member of the Coast Guard that is working with us day-to-day in the development of the requirements with the rest of the services from the Department of Defense, just for your awareness.

Mr. LOBIONDO. Okay. That is very helpful. Thank you.

Thank you, Mr. Chairman.

Mr. SAXTON. Thank you, Mr. LoBiondo.

Mr. Hill.

Mr. HILL. Thank you, Mr. Chairman.

I just have one quick question, and I thank you all for coming. It is a follow-up question to the gentleman from Minnesota.

There is some question as to the quality of some of this equipment. As you probably know, last year the General Accounting Office (GAO) did a study that indicated that a large percentage of this equipment was not ready for the soldiers for them to be protected. I raised this issue with General Myers over at the Pentagon one day, and he acknowledged that there were some problems and that he would work to resolve them and get back with me, which



he did. He wrote me a letter about a month ago asserting that the problems that were there had been corrected.

Recently, several weeks ago, 60 Minutes—I don't know if you saw the piece or not—did another investigation saying that it wasn't up to par, and I would like to get your comments about the GAO study and the piece that 60 Minutes did.

Dr. KLEIN. Let me make a comment first and then let General Reeves comment on specifics.

As you know, with the defense logistics agency handling a lot of equipment and a lot of suits, a lot of activities, it is not 100 percent accurate; and there will be cases where equipment didn't get where it should. We absolutely want to minimize that at all costs. We have a lot of our production lines running at a much higher capacity for the JSLIST suits, so we have taken a lot of proactive actions on that.

A lot of times the programs and news media will pick up on old stories rather than current stories, and General Reeves can talk about specifics, but our troops are protected. The equipment is there. General Reeves can talk a little bit more on specifics.

General REEVES. Sir, there is an old saying in the armed forces, "the command does well what the commander checks on."

One of the things we did as a result of that report is change the status of the readiness reporting to include the chemical and biological defense items that previously commanders only had to report what they had on hand and not if they worked. So we changed that so they had to do both. That gave the command emphasis that was necessary to ensure that that equipment was properly maintained and brought up to standard.

It is up to standard. We set our standards very high, as we should. While you might want to quibble about some of the numbers that were in those GAO reports, the bottom line was we recognize the problem, we have identified it, we fixed it, and that equipment is up to standard.

As far the 60 Minutes report, I believe the specific reference is to a previous generation of protective overgarments called the battle dress overgarment; and, frankly, 60 minutes was reporting old news. These were garments that were made more than a decade ago and made by a company called IsraTech. There was deliberate fraud on the part of that company, and both the President and CEO went to jail.

While there are some numbers that have been reported about potential defective suits floating around the system, the two numbers I would ask you to remember are three and zero. We have checked our inventory three times top to bottom, and there are zero defective suits in our inventory. We do have some of the battle dress overgarments that we know are good that we keep in war reserve and in contingency stocks. We are absolutely certain they are good.

But what is being issued today is not those overgarments. What is being issued today is the Joint Service Lightweight Integrated Suit Technology or JSLIST and sometimes called the Saratoga in the Marine Corps. So we are confident that the equipment we have on hand meets readiness standards and that our soldiers, sailors, airmen and Marines are trained and ready to use it.

Dr. KLEIN. The other activity that has really helped is General Goldfein with his Joint Staff at the Joint Requirements Office looks to make sure that the requirements are met and that they are there. So I think we have added also another layer to make sure we are meeting the needs of the men and women in uniform.

Mr. SAXTON. Jean Reed tells me that the battle dress overgarment has been retired and been replaced and no longer in use.

General REEVES. That is correct. We do keep some in contingency stocks, but at the rate that we are buying new JSLIST suits we expect those contingency stocks will be totally replaced.

Mr. SAXTON. Is that true servicewide or is that specific to Central Command?

General REEVES. That is true to Central Command right now. There are some units that still have the battle dress overgarment as their primary suit but not in the area of operations that we are concerned with today.

Mr. SAXTON. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Actually, Mr. Hill had asked one of the questions that I wanted to inquire about; and I am particularly concerned about the effectiveness of the chem/bio suits since that is the major threat that potentially our soldiers could be facing in theater in Iraq right now. I am reassured by your confidence you have expressed today in the suits.

Beyond that, I would like to know if you have plans to outfit State and local first responders with some of the equipment that is being developed by DARPA or DTRA and to what extent are you working with the Department of Homeland Security to—in assessing the domestic needs for weapons of mass destruction countermeasures?

Dr. KLEIN. On the area of providing equipment to the first responders, unfortunately, we have quite a bit of requirements that we need to meet with the Department of Defense. So it is not likely we will provide them with equipment, but we certainly have supplied them with the technology and what they should buy and how can they can operate.

In terms of getting the technology out from both DARPA and DTRA, all of us work hard to make sure we meet the needs for the Department of Homeland Security. We have joint meetings and I met recently with Dr. McCrery, who has been nominated for Under Secretary for Science and Technology, to make sure he is aware of what we have involved in the Department of Defense that protects individuals.

We have also met with Paul McHale, also with the Department of Homeland Security. So we are very active in trying to let individuals know what the Department of Defense has so they can apply it to the civilian sector.

Dr. YOUNGER. We have a close working relationship with General Eberhardt at Northern Command with responsibility in this area as well.

Dr. TETHER. We are probably doing it the more straightforward way. Some of the people who are working at Homeland Security came from DARPA. They are ex-program managers—recently left

DARPA, so they understand what we are doing, and there is a very close relationship.

Mr. LANGEVIN. Just if I could, on a follow-up on the chem/bio suits, are there things that you can talk about in an open session that you are concerned about where effectiveness would be compromised?

General REEVES. We do not have any concerns, and I believe I understand the reference to what you may be speaking about. We have tested the suit extensively against all known and suspected agents and even some that we don't believe have ever been fielded to assure ourselves that we have both a solid chemical and biological capability.

Mr. SAXTON. Jim, you have about another two minutes. We missed the clock up here. If you have another question, fine. If not, we will move on.

Mr. LANGEVIN. I will submit questions later for the record.

Mr. SAXTON. Mr. Wilson.

Mr. WILSON. Thank you very much for being here today.

I was looking forward to this hearing, but I was also dreading this hearing because the summaries indicated, I think correctly, that the greatest uncertainty that U.S. Forces have is the potential of biological weapons, chemical weapons and their use in a widespread nature. And I really have been very concerned for our troops. But the information you provided today is so encouraging.

I have been to a number of departure programs and ceremonies and, seeing the Army and Air Guard troops departing, my major concern for all of them and for their families was the potential of chemical and biological attacks. But what you have said today is extraordinary, and I certainly hope this gets wide play.

Because my familiarity with this is wearing mock gear not ten years ago but two-and-a-half years ago at the National Training Center in the Mojave Desert, and the mock gear I had was antiquated compared to what you just showed. The lightweight nature of it, the gas masks themselves appear, again, much better than anything I have ever seen; and so I am very, very encouraged.

Then to find out that you have had 20,000 chemical detectors in theater—and that is just wonderful—and 19 new systems in place since the Persian Gulf War, I think this is so reassuring for families. In fact, I would like for you to maybe restate again for the families of service members, particularly General Reeves and if anybody else would like to chime in, what message would you like to give to families who have young people who are in harm's way today as to the capabilities that you have previously provided to us?

Also, I want to make sure you indicated that all troops have this capability; and I want to make sure it includes guard and reserve units.

General REEVES. You would be correct. They have the new protective mask. They have the new protective suit.

What do you tell mom and dad at home? That is an important question. What you tell them is that the unknown is not a very comfortable place sometimes and can be a little bit scary and sometimes experience you get 10 minutes right after you need it. What we do from the very first moments that our soldiers, sailors, air-

men and Marines enter basic is introduce them to how to use this mask. We then build that experience into their individual and advanced training.

As you mentioned, we take them places like the National Training Center that is in the Mojave Desert; and we give them more experience and comfort with this equipment. But, most importantly, we give them confidence that this equipment works. I have personally worn this equipment in a live chemical agent environment. So have 70,000 other soldiers, sailors, airmen and Marines without a single incident. It works. I would trust my family's lives. I would trust my daughters wearing this equipment to protect them. The parents and brothers and sisters who all have loved ones in the area of operations should have every confidence that their soldiers, sailor, airmen and Marines are trained, they are ready and their equipment is world class.

Dr. KLEIN. One of the things that I have been very impressed at the Department of Defense is when you work in the Pentagon and you meet a lot of the young men and women in uniform you soon realize that you are not sending a mysterious individual there, you are sending a real person. All of us at the table take our job very seriously. We work extremely hard to make sure that the men and women that are forward deployed are the best protected that they possibly can be. Because just like people that vote for you, people that we work with within the Pentagon are people that we know are forward deployed, so we work very hard.

I think—as General Reeves said, I think we have the best trained and equipped chemical, biological and defense system anywhere in the world. Is it perfect? Probably not. But it is the best we can have available, and we have all put a lot of hours in to make sure that that happens.

Mr. WILSON. I want to thank you again on behalf of moms and dads and spouses, family members. This is just so reassuring.

It adds to the fact—I was in Kuwait and saw the units from the Czech Republic, and it is exciting to see their active involvement. I understand Romania has been providing personnel for chemical and biological efforts and working together.

This is so reassuring to families, and I appreciate what you have done and the vision that you have placed into this.

I yield the balance of my time.

Mr. SAXTON. Ms. Davis.

Ms. DAVIS OF CALIFORNIA. Thank you, Mr. Chairman.

Thank you all for being here and for your service.

Just a quick follow-up, are there any other priority requirements that we have for improving the capabilities of our servicemen and women in the Middle East? You mentioned sensors, the protective gear. Is there anything else that is essential and important to that?

Dr. KLEIN. I believe that the forward-deployed troops are the best protected that they can be. Are there things that we wish we had that we didn't? Absolutely yes. We wish we had better send-off detectors. We wish we had better antibiotics. We wish we knew what was coming so that we could detect to prevent rather than detect to treat. Our forward-deployed troops are trained, equipped and ready to roll.



Ms. DAVIS OF CALIFORNIA. Are there efforts in that realm of the more proactive response to the elements? Are we working on that? Where is that coming from? And how can we be supportive?

Dr. KLEIN. Probably on the detectors is one of the most active programs that I have seen. We all get calls periodically from people who have the best detector, better than sliced bread, that has come out. So there are a lot of people working on detectors, both in the Department of Defense and out. We have organized programs both within the chem/biodefense program through DARPA. Some of the Department of Energy (DOE) national labs are also working on detectors.

Ms. DAVIS OF CALIFORNIA. If I may follow up quickly with the time constraints, I know that in San Diego we have a wonderful collection of industries and businesses that are part of the folks who are knocking at your door with these extraordinary new sensors, and what I know from some of their experiences is that it is very frustrating to get attention. How do you suggest we do that? We all probably have folks in our district who have some—what may seem like an extraordinary contribution to make, and they are pretty frustrated.

Dr. KLEIN. Not that I am looking for more mail. However, if someone has a detector that has the appearance of providing the Department of Defense beneficial applications, contact me. I will then send it to the right people. We will have it evaluated.

One of the difficulties that I think industry has—and I really saw this when I was teaching at the university. An individual will come up with an idea, and they think that is it. You know, once they come up with the idea, end of discussion. But that is when it begins. Because you have to make sure you have a prototype that has been tested, it is funded, and it can be manufactured.

I think part of the frustration on some of the companies are that the Department of Defense has a requirement to test. It is not acceptable for us to deploy men and women into potential hostile areas and not be assured that this equipment will work. So I understand part of their frustration, but we cannot always rely on the company's data for test performance. We have to verify and test so we can be assured that our men and women are protected. I understand the frustrations, but they have to understand what our responsibilities are.

Ms. DAVIS OF CALIFORNIA. Is there a process so that they know there may be an opportunity to look at that, they might hear within a three-month period of time? I think that is partly—what kind of feedback do they get that is part of the problem?

General REEVES. If I may, since it is kind of an opportunity for an advertisement, the 7th through the 9th of April we in fact are doing an advanced planning briefing for industry right in Hunt Valley. It is sponsored by the National Defense Industrial Association. It is on the web; and it is where we invite contractors to come and listen to what we are doing, everything from the science and technology base, the kinds of things that are being done in basic technologies, the whole way through, what our plans are over the next two to three years for procuring new equipment so that industries have the opportunity to see what is in the program and have the opportunity to make their business plans accordingly.



The second thing we do is, once a year, we run something called a technology readiness evaluation; and this is a pretty good deal. It is an opportunity for—based on whatever the particular test is that we are running—companies in that particular sector to come and have their equipment independently tested normally at Dugway Proving Grounds. We frequently do it with live chemical agents or live biological agents, obviously in a very contained facility with appropriate safety precautions as well as out in an open range.

The quid pro quo is that we get to keep the data so that we can see how mature that technology is so that, when opportunities present themselves, we know that company exists, we know the maturity of that technology; and if we need it in a hurry, we can reach out and get it.

General GOLDFEIN. I might also add, since the formation of the Joint Requirements Office, since the short time we have been operating, I have a number of calls and had folks come in. One was a university group that came up with an idea about how you can do medical surveillance. What I mean by that, as doctors are seeing patients, perhaps at the early end of a situation, they are beginning to pick up certain symptoms. If you had a system that is tracking that, perhaps you begin to pick up the idea of what might be out there earlier than an individual doctor could.

So they take that idea and bring it in to us. I would speak with my colleague. We would talk with the Joint Forces Command and their experimentation role, and we begin to look for ways the team can come together. I have seen a couple of those. One happened to be a detection system from your part of the country as well.

So I think we have had a number of different ways and angles that people have been able to introduce their thoughts, and we welcome them.

Ms. DAVIS OF CALIFORNIA. Thank you. Appreciate it.

Mr. SAXTON. Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

Dr. Younger, I was reading an article in the New York Times entitled, Teams of Experts to Hunt Iraq Arms. This article describes the mobile labs that have been assembled. I believe two are referred to in the article that can analyze chemical and biological samples in less than 24 hours with 90 percent confidence being sent recently to Kuwait. Your agency, the Defense Threat Reduction Agency, is charged with carrying out this effort that is being made; and I noticed in the article that it stated that you had only been officially charged with the responsibility for carrying out this mission two weeks ago.

My question is, recognizing the importance of being able to identify and disable any unconventional weapons that we find in Iraq, why did your agency only get the official charge to carry out this mission just two weeks ago?

Dr. YOUNGER. Congressman, we have been working on this far longer than two weeks. Indeed, that is the reason DTRA—for the existence of this agency. We have had intense efforts on this for some time. We have been working very closely with Central Command in preparing plans related to WMD operations for potential operations in Iraq.

The reference to an event of 2 weeks ago, I will be delighted to talk with you in another setting about. I am not free to share that at this time. But we have been actively engaged in that for some time.

Mr. TURNER. Dr. Tether, you certainly have an excellent reputation at DARPA for advancing the use of technology in the defense of the country, protection of our troops and other endeavors important to our national defense. I recently heard that the new Department of Homeland Security was contemplating the creation or has created a similar agency.

I would like to ask you to give us the benefit of your experience on an issue that has been quite troublesome to me. That is, we have seen a whole host of private-sector companies coming forward with various solutions that they want to offer up to the government to solve the problem of homeland defense. I had in my office the other day a company who says they are on the verge of the solution to anthrax, and I am sure you are familiar with their proposals. But I am looking for your suggestions on the best way to organize the government to ensure that we are able to have the private sector clearly know where they go first with their ideas and how should we be organized as a government to look at those ideas to review them, to determine whether they should be looked at closer, to then process that so that the best ideas that the private sector is offering can float to the top, be identified and then be deployed in the defense of our homeland.

Dr. TETHER. How should the government be organized? Thank you for asking the question.

Mr. TURNER. Didn't want to give you a softball here.

Dr. TETHER. Yes, they are forming an organization in the Homeland Security model directly after DARPA. I think they call it SARPA, Homeland Security Advance Research Projects Agency. There are several ex-program DARPA managers who are involved with that organization, and deliberately so, to give it the flavor of DARPA.

DARPA was created roughly 44 years ago to basically reach out and find those people who had ideas that weren't in the common way of thinking, ideas that people that were counterculture—that were against current concepts or against current systems. We have been quite successful in doing that, and I believe the Homeland Security Department is going to try to emulate that as much as they can.

Now how to describe what we do. It is a small organization, and we have 150 program managers. They are only there for a very short time, four years, five years. There are no careers at DARPA. In fact, there are no jobs at DARPA. We hire people for their ideas, and they know they have a short period of time, and they go out and find the best people in the world to execute those ideas.

We also have the capability at DARPA to contract very quickly. All of these have actually been given to us by you all. You have given us a great deal of authority to contract very quickly. I think you have done the same thing to the Homeland Security people. We have given them the ability to have what is known as "other transactions."

People know that if they have an idea and they don't want to wait a year to try to get it funded, they want to get a fair hearing, they come to us. How do they learn to come to us? It has been 44 years.

Now, hopefully, we are going to try to help the Homeland Security people in the same way in trying to help them—mainly because I get a lot of people that come into my office with the same question, and I am trying to shift them over—and they are very frustrated, and they don't know who to go to have—buy their equipment. If I were the same companies, I wouldn't know who to go to. Who do you go to have local and State first responders buy the equipment? I don't know the answer to that question, and I am hoping that the Homeland Security people will be the ones that will be able to do this.

It is not us, the Department of Defense. We know how to buy very well for our forces. But how to buy for a police Department that has maybe ten policemen, we really don't know how to do that. But we are trying to give them the methodology at DARPA.

I almost hate to say it, but DARPA is really an organization of mavericks. We believe that you read something and if it says you can't do it, then you can do it, as opposed to looking to see what it says you can do. That is just the nature of the organization. I always say that DARPA program managers have two jobs, one, to get the best ideas; and they should always be trying to get the DARPA director fired for something or another. Unfortunately, my guys seem to be doing a pretty good job of that at times.

I know that doesn't answer your question totally. I don't know the answer, but I know our process works and our environment, and we are trying to make it be the same thing for the Homeland Security people.

Dr. KLEIN. As you probably know, there is no single silver bullet that answers all of those questions, but some of the things that you have done in Congress has certainly helped.

For example, in fiscal year 2003 you provided a \$25 million chem/bio initiative. There is nothing like money to get the creative juices flowing for a lot of our scientists and researchers out there. So when you have an announcement that there is funding available for certain missions, that gets people's attention and lets you know to where to go for those tasks.

So Congress has also played a role in getting the word out in a variety of areas, and I am certain for the Department of Homeland Security they will have similar broad initiatives that will also get people's attention.

Mr. SAXTON. Thank you very much.

Mr. Bartlett. Our inventor, Mr. Bartlett.

Mr. BARTLETT. Thank you very much.

I am sorry I missed the first part of the hearing, and maybe my concern has been addressed.

I understand that for about the last decade we have been waiving chemical hardening on essentially all of our weapons systems procurements. Has that been a consideration and a concern?

Dr. KLEIN. We have—on a lot of our equipment, we have radiation hardening on a lot of the equipment; and we certainly need to address that as we move more and more to buying things off the



shelf. For equipment that is sensitive to radiation, we need to make sure we have radiation hardening.

Mr. BARTLETT. We have also waived radiation or Electro-Magnetic Pulse (EMP) hardening, but it is my understanding that we have waived chemical hardening on this equipment. Do they tell you when you get the equipment in the field to what specs it has been built so that you know whether it is radiation hardened or chemically hardened?

Dr. KLEIN. I can tell you, and then I will let General Reeves add a little bit more. But in terms of using decontaminants, if a piece of equipment is contaminated, we do have procedures where we test the decontaminant solution and things of that nature; and I will let General Reeves add a little bit more on what happens in the field.

General REEVES. There is a two-part answer to your question.

First of all, we do have a resistant coating on our equipment in the field, the so-called CARC coating, or chemical agent resistant coating, which is a special paint that we put on all of our vehicles specifically designed to resist attracting or retaining chemical agents and to aid in the decontamination. So in terms of the exteriors of the vehicles, we have done nothing to relax that.

Now when it comes to things like sensitive equipment, electronics, absolutely. We have not made any attempts for pure economic reasons to harden all of those electronics against a chemical agent. Instead, we have proposed and the Congress has been kind enough to fund a program we call the Joint Service Sensitive Equipment Decontamination Program, where we are looking at decontamination solutions that allow us to decontaminate a variety of sensitive equipment so that we can get the best of both worlds, quite frankly. We can take the economic advantage of being able to buy commercial off the shelf and still have systems that we can decontaminate.

Mr. BARTLETT. Do we have any ideas of the vulnerability of our equipment to chemicals that might be used, and do we have assessment of the vulnerability of our equipment to the decontamination procedure which are also chemical procedures?

General REEVES. I understand your concern. The corrosive decontaminants of old DS-2, where we frequently had a successful operation but the patient died because it was so corrosive, is not what we are using today. We are using an environmentally benign yet effective decontaminant called DF-200. It is a liquid. It allows us to decontaminate equipment without affecting it and provides a much better situation for the environment once you have neutralized what is on that equipment. So we are much more comfortable with the decontaminants we are using today than we were just even a few years ago.

Mr. BARTLETT. Do we have any assessment of how much of our equipment may not work after a chemical attack because it has not been chemically hardened in its manufacture?

General REEVES. To my knowledge, no. Because the equipment, frankly, from a nerve vapor may be contaminated, but it doesn't mean it won't work. The equipment simply needs to be decontaminated as quickly as possible. There is very little in the vapor that

would cause anything—particularly electronics and those kinds of things—that would cause the same particular issue.

Mr. BARTLETT. I am not certain what chemical hardening means. All I know is, for about a decade, we have waived it on essentially all of our weapon systems procurements; and this gives me a nagging concern that some of this equipment on which we rely might not be available to us after a chemical attack. It is not just that the equipment would be contaminated and, therefore, if you touched it, you would be contaminated, but my understanding is that you chemically harden the equipment so it will work in the face of a chemical attack, and it is my understanding that essentially none of our equipment for the last decade has been chemically hardened. Is that a correct assumption or do you know?

General REEVES. I believe it is, because the survivability requirements that we have primarily refers to the nuclear hardening requirements. We recognize that we can decontaminate equipment and that the vapor itself in a hardening sense really is not an issue.

Mr. BARTLETT. Thank you, Mr. Chairman. I would hope that for the future that there would be some prohibition against waiving hardening for weapons that might indeed be used against our people and their equipment. Thank you very much.

Mr. SAXTON. Thank you, Mr. Bartlett.

Dr. Klein, the previous administration attempted to abolish your office, the Assistant to the Secretary of Defense for Nuclear, Chemical and Biological Programs, a position called for by statute. Congress refused to accede to the request. However, the position was vacant for over 45 months and other officials were dual-headed to fulfill the statutory position. How does your confirmation and appointment as the Assistant Secretary of Defense for nuclear, biological and chemical (NBC) help to address nuclear chemical and biological issues faced by the Department of Defense?

Dr. KLEIN. When I look at the hours I put in every day, it amazes me that the position went unfilled as long as it did.

It is a subject that obviously is very near and dear to Congress and certainly to the Department of Defense and weapons of mass destruction. I think in my position being filled, what I hope I have added is a focus and a vision.

One of the difficulties we have is the people we have that work in the Pentagon are excellently trained. They really do a good job, but they are involved in so much day-to-day activity that—in doing their job that it really takes, I think, someone at the Presidential appointment level that should look at the focus and vision and where should we be in 10 years, 20 years and 30 years and then how should we get there.

The other advantage it has for having the position filled is that any time you have a newcomer come in they ask questions, is there a better way to do it? So I would hope that my position, having now been filled, has added value; and I can tell you from the hours that I put in I think there were things that were just not getting done in the past.

Mr. SAXTON. Some have proposed consolidating the chemical and medical and biological defense program under the DOD medical



community. What are your views on the proposal of this consolidation?

Dr. KLEIN. Mr. Chairman, the first thing that I do is I follow the law. There is currently a law that says how the chemical and biological and defense program is organized, and we intend to follow that law. We have very close cooperation in keeping the medical community informed. We are reorganizing the chemical and biological defense program to make it more streamlined. More people are accountable.

DTRA will be tasked with organizing the science and technology part of that program. That includes medical and nonmedical. On the medical side, we will have a physician that leads that effort.

So I believe, right now, with the way the program is organized, not only does it meet the law, it meets the intent of the law.

Mr. SAXTON. I understand that the statutory—I understand the statutory provisions. However, the proposal would be for us to consolidate through an authorization provision in the defense bill this year the chemical, biological, medical defense program—whether under the DOD medical program—would you favor that? Think it is a good idea? Or do you think that we are better off staying with the status quo?

Dr. KLEIN. I have not seen the official proposal, but I believe from my perspective I would like to see how our new streamlined chemical, biological and defense program works. Organizing and implementing—then I think we should come back and tell Congress where the weaknesses are.

Mr. SAXTON. Okay. We hear you.

Listen, thank you, Dr. Klein, for spending this time with us. We have been at this for about an hour and 40 minutes, and we appreciate your participation as well as the experts to your left and right. We have enjoyed listening today and last week and earlier this week as well to the gentlemen particularly to your left; and we appreciate the good work that all of you are doing.

The advances that have been made and the technology that has military application in many instances are astounding. Mr. Wilson was telling me as we were sitting here how pleased he is to see the chemical and biological protection that our forces have. We were absolutely astounded at Dr. Younger and Dr. Tether's presentation late last week and early this week. So thank you for the job you all are doing. We appreciate it, and I am sure the troops and the family of the troops that benefit from the technologies that you have collectively provided feel the same way.

Thank you for being with us. We look forward to working with you in the future.

The hearing is adjourned.

[Whereupon, at 3:40 p.m., the subcommittee was adjourned.]



---

---

# **A P P E N D I X**

MARCH 19, 2003

---

---



---

---

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

**MARCH 19, 2003**

---

---





OPENING REMARKS OF JIM SAXTON  
CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES SUBCOMMITTEE  
HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE HEARING  
"COUNTERING THE THREAT OF WEAPONS OF MASS DESTRUCTION -  
DEPARTMENT OF DEFENSE POLICY AND PROGRAMS FOR FISCAL  
YEAR 2004"  
MARCH 19, 2003

THE COMMITTEE WILL COME TO ORDER.

GOOD AFTERNOON. TODAY THE SUBCOMMITTEE ON  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES MEETS  
TO RECEIVE TESTIMONY ON DEPARTMENT OF DEFENSE POLICY AND  
PROGRAMS FOR COUNTERING THE THREAT OF WEAPONS OF MASS  
DESTRUCTION.

THIS HEARING COULD NOT BE MORE TIMELY. WAR WITH IRAQ  
IS IMMINENT AND OUR ARMED FORCES AND THOSE OF OUR ALLIES  
WILL FIGHT UNDER THE THREAT OF POSSIBLE USE OF CHEMICAL  
AND BIOLOGICAL WEAPONS BY OUR ADVERSARY. TERRORIST  
GROUPS HAVE ACTIVELY SOUGHT TO OBTAIN THE CAPABILITY FOR  
USE OF CHEMICAL, BIOLOGICAL, RADIOLOGICAL, OR EVEN NUCLEAR  
WEAPONS AND WOULD POSE THE USE OF SUCH WEAPONS TO  
ACHIEVE THEIR OBJECTIVES.

WEAPONS OF MASS DESTRUCTION – NUCLEAR, BIOLOGICAL, AND CHEMICAL – IN THE POSSESSION OF HOSTILE STATES AND TERRORISTS REPRESENT ONE OF THE GREATEST SECURITY CHALLENGES FACING THE UNITED STATES. IN MEETING THIS CHALLENGE THE DEPARTMENT OF DEFENSE PLAYS MAJOR ROLES, BOTH WITH RESPECT TO THE CAPABILITY OF OUR ARMED FORCES AND THE SUPPORT THE DEPARTMENT PROVIDES TO HOMELAND DEFENSE.

THE PURPOSE OF TODAY'S HEARING IS TO GAIN AN UNDERSTANDING OF THAT ROLE AND THE DEPARTMENT'S ORGANIZATION, POLICY, AND PROGRAMS FOR COUNTERING THE POTENTIAL THREAT OF WEAPONS OF MASS DESTRUCTION AND FOR ENSURING THE CAPABILITIES OF OUR ARMED FORCES TO FIGHT ON A BATTLEFIELD UNDER THE THREAT OF THE USE OF SUCH WEAPONS.

TO ADDRESS THESE ISSUES WE HAVE AS OUR WITNESSES TODAY:

THE HONORABLE DALE KLEIN, ASSISTANT TO THE SECRETARY OF DEFENSE (NUCLEAR AND CHEMICAL AND BIOLOGICAL PROGRAMS);

THANK YOU CONGRESSMAN MEEHAN.

DR. KLEIN, YOU MAY PROCEED.

**Opening Statement of**  
**The Honorable Martin Meehan (D-MA), Ranking Member,**  
**Subcommittee on Terrorism, Unconventional Threats**  
**And Capabilities**  
**March 19, 2003**

Thank you, Mr. Chairman. Let me, first, thank you for scheduling this hearing; and, second, let me also join you in welcoming the distinguished members of this panel. Gentlemen, thank you for being with us this afternoon.

Mr. Chairman, like you, I believe the issue before us today is of the utmost importance. No other effort should receive more attention than that devoted to countering the threat of weapons of mass destruction (WMD). No less than 25 nations currently possess the means of WMD, and a real threat exists for these instruments of destruction to fall into terrorist hands.



As we'll hear today from our panelists, countering the WMD threat involves more than simple investments in technology development. Indeed, countering the threat requires a comprehensive and all-encompassing approach, one involving both technology development and nonproliferation initiatives. Securing diplomatic agreements, arms control measures, and other threat reduction efforts often hold as much – if not more – promise as the pursuit of technology development. In truth, a coordinated approach tempers the technological challenge facing our nation's scientists – it is the "Threat Reduction" part of DTRA (pronounced DITT – RUH).

That said, I hope the panelists today will help us better understand the unique challenges involved in our effort to confront the chemical and biological threat. I understand the threat is unique. Yet I also understand that we are pursuing several different approaches to reduce, eliminate, or secure WMD sources. I look forward to hearing about them in greater detail.

Mr. Chairman, again, I join you in welcoming the witnesses today. I look forward to their testimony.

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

STATEMENT OF  
DR. DALE KLEIN

DEPARTMENT OF DEFENSE

MARCH 19, 2003

BEFORE THE  
SUBCOMMITTEE ON TERRORISM,  
UNCONVENTIONAL THREATS AND CAPABILITIES

COMMITTEE ON ARMED SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

Statement of

Dr. Dale E. Klein

Assistant to the Secretary of Defense

for Nuclear and Chemical and Biological Defense Programs

March 19, 2003

Committee on Armed Services

United States House of Representatives

Chairman and Distinguished Members: I was appointed by President Bush in November 2001, following Senate advice and consent, to my present position. Within the Department of Defense, I have responsibility for all matters concerning the formulation of policy and plans for nuclear, chemical and biological defense programs. However, I will focus most of my remarks on chemical and biological defense programs rather than on my nuclear responsibilities. While the committee has asked our panel to appear in the connection of terrorist use of Weapons of Mass Destruction (WMD), our concern includes any WMD threat against our women and men in uniform. It is not just enough to consider terrorism—we must also consider traditional acts of war, industrial or transportation accidents, weather-induced releases, operator errors or other potential predicates for WMD release. The warfighting commander does not need to consider if a trucker failed to close a valve or if lightning struck a toxic industrial chemical storage site or if al Qaeda operatives are releasing toxins near an overseas base. In each case, the warfighting force needs protection. The experts before you today develop technology solutions; work on new concepts to improve tactics, techniques, and procedures; provide WMD combat support expertise; and manage the fulfillment of our chemical and biological defense equipment requirements with the industrial base of our nation and our allies. Due to the support of the Congress and with the help of the resources you have made available to the Department; our fighting

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

forces are equipped and trained far better than in 1991 during OPERATION DESERT STORM. The priority placed on, and concern taken with, chemical and biological defense shows a focus at a high level. In fact my boss, Pete Aldridge, commented that for a period of time, he was spending more of his personal attention on anthrax vaccine than on the Joint Strike Fighter which may become the largest program in DoD history! I want to assure members and our citizens we are supporting our troops and that the equipment they will use has been designed and tested to withstand enemy chemical or biological attack. Our logistics experts have made sure that the right equipment has been supplied to the right units at the right time. Commanders have conducted numerous training drills simulating WMD attacks and our troops have practiced their individual protection actions. I am confident we are as ready as we can be given the technology available today.

Congress has called for and we have delivered on a number of initiatives which significantly improve our ability to protect our fighting forces in the field, at sea, or in the air. We have improved detection and identification technologies; individual protection systems; decontaminants; biological medical protection; and, warfighter awareness of the threat. Our commanders in the field have the benefits of those improvements. I will describe, in specifics, Force Protection Initiatives, Biological Detection Capabilities, Chemical and Biological Protection Ensembles and Biological Defense Vaccines.

**Force Protection Initiatives**

In fiscal year 2003, \$32.9 million was allocated for installation protection equipment within the Chemical and Biological Protection Program. The Chemical and Biological Installation Protection Equipment is an integrated suite of highly effective sensors and related equipment to be installed at nine stateside military installations. The equipment suite will provide tiered sampling and collection, detection, identification and warning capabilities. It is designed to provide early,

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**



**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

indoor and outdoor collection, detection, presumptive identification, and warning. Confirmatory identification and enhanced medical surveillance capability is also included.

In the Fiscal Year 2004 President's Budget, we have requested a significant force protection initiative. This program will provide chemical and biological protection coverage to 200 DoD installations. This protection will include sensors to detect radiological threats. The equipment to be deployed will be integrated in the base operational command and control infrastructure. Bio-detection equipment will consist of automated Joint Biological Point Detection Systems and Portal Shield systems along with manual dry filter unit samplers. Support from laboratories will consist of tiered, multi-technology, confirmatory testing protocols. Chemical detection will be provided by Automatic Chemical and Agent Detector Alarms and the Joint Chemical Agent Detector integrated with base command and control systems. The program will procure initial detection agent consumables, new equipment training, spares, contractor logistics support and operators.

**Biological Detection Capabilities**

Aside from a sick person requesting medical aid, biological detection capabilities available in 1991 were very limited. The primary system available included assays that were manually operated, capable of detecting only a few pathogens and were susceptible to false readings. Over the past several years, the Department has fielded several new biological detection capabilities. With the Army's Biological Detection Companies, the Biological Integrated Detection System or BIDS, will provide a multi-technology point detection system. The Navy has installed the Interim Biological Agent Detector on ships deploying to the Persian Gulf. In addition, we have fielded the Portal Shield network sensor system for protection of critical fixed sites. We have also fielded the Biological

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

Weapon Sampling Kit which includes hand-held immunochromatographic assay, a simple, antibody-based test used as a quick screen to presumptively identify biological agents from environmental samples. The M93A1 NBC Reconnaissance System provides a variety of capabilities including the new Chemical and Biological Mass Spectrometer and improved warning and reporting systems to reduce reaction time throughout the theater.

The comment I heard on my first visit to the field and one I have heard frequently, involves the need for standoff detection of biological agents. I want to be especially candid: the problem of stand-off detection of biological pathogens in near-real-time remains an extremely difficult challenge. We can detect many important kinds of dangerous radiological and chemical threats at stand-off distances in near-real-time. However, there are many interfering biological signals present in the environment; we must be able to distinguish between the dangerous and benign strains; and we will have to determine if threat organisms will remain viable and pathogenic as they traverse the space between their current location and the deployed military force. We are investigating techniques such as multi-spectral laser-based technologies to provide earlier warning to our warfighters.

**Chemical and Biological Protective Ensembles**

Beginning in 1996, an improved individual protective ensemble known as the Joint Service Lightweight Integrated Suit Technology (JSLIST) first became available. JSLIST, or in Marine parlance, Saratoga, replaced the Battle Dress Overgarment (BDO), used in OPERATION DESERT STORM, as our first choice in individual protection. While BDOs remain fully effective and available as a backup, they are heavier than the JSLIST. My wife actually wore the BDO during her service in OPERATION DESERT STORM. She told me the carbon protective element of the BDO would leak through the inner liner and provide a thin and unattractive coating of black dust on her skin. This characteristic didn't

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

make wearing the BDO popular! The JSLIST provides a greater duration of protection once presented with a chemical threat and it may also be laundered. As you know, the Department discovered defective BDOs purchased before the JSLIST became available. We were able to locate 600,000 defective BDOs before issue to units. All units were advised to use the remaining, already distributed, defective BDOs for unit training use only and remove them from war reserve stocks. Three different times, the Army has tasked units to search for and remove from war reserve stocks any defective BDOs identified by lot number. Much has been made of the possibility that defective BDOs remain in the logistics pipeline because we did not account for every defective BDO as it was used in training. While I cannot fully eliminate the possibility that in a locker somewhere there might be a small handful of defective BDOs, I believe the possibility is quite low and I am confident this issue has been resolved.

Since initial fielding, there has been increased emphasis to field JSLIST to the entire force and to phase out the BDO entirely. Our procurement strategy, supported by Congressional authorization and appropriations, has permitted the Department to ensure that all of our forces in the region will have two JSLIST each and Marines will have three each. Continued production in JSLIST procurement is needed to fully replace the BDO, and to replace any JSLIST used if hostilities occur.

The Department is committed to improving the design of the JSLIST. We are investing in our science and technology base to find non-carbon based materials to reduce weight and thereby improve comfort and mobility. We are attempting to develop self-detoxifying clothing that will allow our personnel to better sustain operations in a contaminated environment with reduced risk. Additionally, improved masks and filters are being designed to increase protective margins, improve visual awareness, and improve weapon system compatibility.

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

**Biological Defense Vaccines**

Medical protection is crucial to military operations and success in the field. In 1991, we had very limited stocks of vaccines and no way to surge production. Currently we have a Food and Drug Administration (FDA)-approved production line for anthrax vaccine. FDA approval was not obtained without a strong effort by both the government and the contractor members of the team. All deploying forces receive smallpox and anthrax vaccines. DoD supplies anthrax vaccine to other federal agencies once DoD requirements are fulfilled. The Joint Vaccine Acquisition Program is working to fulfill defense biological vaccine requirements including maintenance of a military vaccine stockpile. The Department is working with the private sector, the Department of Health and Human Services, and the Department of Homeland Security to establish a national approach to assured vaccine supplies both for homeland security and homeland defense missions.

**Summary**

DoD places a very high emphasis on protecting our warfighters from chemical and biological agents. We are ready for combat operations in southwest Asia. We are working many approaches: arms control, cooperative international programs, combat operations, and consequence management operations, to name just a few. We intend to reduce, eliminate, or secure WMD sources. We will predict, detect, and interdict the transmission of WMD to the extent possible. Finally when we are targeted, we will protect our people and facilities and follow with effective decontamination. We are better prepared on all fronts: battle management, contamination avoidance, individual and collective protection, medical countermeasures, and decontamination. We deeply appreciate the support of the Committee and the members and we are grateful for the sacrifices of our troops, their families, and our coalition partners.

**FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE**

**NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE**

**Statement by**

**Dr. Tony Tether**

**Director  
Defense Advanced Research Projects Agency**

**Submitted to the**

**Subcommittee on Terrorism, Unconventional Threats and Capabilities  
House Armed Services Committee  
United States House of Representatives**

**March 19, 2003**

**NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE**



Mr. Chairman, Subcommittee Members, and staff: I am Tony Tether, the Director of the Defense Advanced Research Projects Agency (DARPA.) I am pleased to appear before you today to discuss DARPA's research to counter the weapons of mass destruction (WMD) that our nation faces today.

At DARPA, our primary area of emphasis in countering WMD has been biological warfare defense (BWD) research, work that we began in earnest in the mid-1990s when it became clear that the threat of biological attack was growing sharply. DARPA moved out ahead of the threat by establishing a comprehensive, aggressive, and innovative BWD program. DARPA's work complements mainstream Federal and commercial BWD efforts. However, DARPA does not constrain its work to the Validated Threat List published by the Defense Intelligence Agency because our enemies will not necessarily stick to the validated list. It is important to also work on "non-validated" threats that could pose a great danger to our forces. This lets us pursue general solutions to the biological warfare (BW) problem, including the worrisome threat from genetically engineered pathogens.

A framework for discussing BWD is to consider the different stages surrounding a biological attack. These stages tell us what we need to do and when we need to do it – that is, what technology we need and what research we need to invest in.

- *Prior to a BW attack*, we need to boost our people's immunity and the effectiveness of vaccines and, if possible, do all we can to keep an attack from happening in the first place.
- *During an attack*, we need sensors to determine its nature – including what agent was used and who was exposed – to set the stage for our response.
- *In the minutes and hours after an attack*, we need immediate ways to protect our people.
- *In the hours to days after an attack*, we must coordinate the first responders and manage our medical system. During those same hours and days, we must begin to diagnose and treat the victims.
- *And in the days and perhaps years after an attack*, we must decontaminate the attacked area.

Let me take these stages one by one, and give you a sample of what DARPA has been doing in each.

### **Prior to an Attack**

Let's begin with the time *before* an attack. Obviously, our number-one priority is to try to prevent an attack from occurring at all. We want to discover the plan for an attack and then take action to disrupt it before it can be carried out. This requires good, actionable intelligence, and DARPA's Information Awareness Office (IAO) is focused on developing the tools to ferret out terrorists' plans. IAO's programs have been the subject of recent controversy, and, since their scope is counter-terrorism in general, rather than specifically focused on countering WMD, I won't discuss them in detail today. But IAO's activities are all about "connecting-the-dots" to uncover planned terror attacks and prevent them.

To protect our people from an attack before it occurs, we have been working with considerable success on a compound called CpG. CpG boosts the body's natural immunity to disease, essentially by priming the immune system to mount an aggressive defense, which could be of great use to first responders. And, it can be used as an adjuvant to dramatically improve the effectiveness and speed of vaccines. For example, animal tests have shown that by combining anthrax vaccine with CpG, we need less vaccine and fewer doses while achieving faster protection with fewer side effects. CpG is part of our comprehensive effort to take anthrax "off the table" as a threat. I will talk more about anthrax later, but we think CpG will prove useful against many other pathogens. We expect to begin human trials of CpG with the current anthrax vaccine this summer.

### **During an Attack**

First, I'd like to talk about sensors. The ideal sensor would specifically identify individual pathogens across the entire range of pathogens, including previously unknown ones, and it would be very fast. Moreover, it would be small, inexpensive, lightweight, and low-power. Unfortunately, as you might guess, these qualities tend to be in conflict with each other, and tradeoffs are necessary. Hence, we need a whole family of sensors – different ones optimized for different purposes. For example, to protect people from being exposed during an attack, *speed* is paramount to protect first and only later figure out what the pathogen was. On the other hand, if

an attack has already happened and people have been exposed, *specificity* is paramount, because we need to determine exactly what people have been exposed to so we can immediately begin administering the right treatment. Another issue is the false-alarm problem, which varies with the specific environment in which the sensors are used and whose severity depends on the steps taken in response to an alarm; in both aspects, military and domestic applications differ widely. Across this complex trade space, DARPA has been working since the mid-1990's to develop a family of sensors that systematically meet these challenges.

A number of our sensors have been picked up by the Military Services and are being fielded or are close to being fielded. DARPA developed a biosensor microarray for rapid identification of biological warfare agents. Like computer chips, which perform millions of mathematical operations per second, DARPA's microarray biochips can perform thousands of biological reactions in a minute with great sensitivity. Moreover, these biochips can be reused up to 50 times, effectively reducing their cost to about \$1.00 per use. These biochips have been transitioned to U.S. Army Soldier and Biological Chemical Command for further testing against live biological agents.

We are all familiar with how canaries were used in coal mines to test the air. DARPA has been pursuing a similar approach, except in our case the "canary" consists of cells on a chip. Cells, of course, do not like being exposed to pathogens, and they are very fast and very sensitive indicators of a problem. Tests have shown that these chips can detect as few as 10 to 50 viruses or bacteria in only 10 to 20 seconds.

A more recent sensor program is TIGER (Triangulation Identification for Genetic Evaluation of Risk). TIGER is trying to develop a universal sensor that can detect any type of pathogen – even unknown and engineered ones – through an innovative method of measuring and weighing nucleic acid sequences. TIGER involves integrating data from multiple regions along an organism's genome to derive a unique identifier for that organism. This should enable us to detect and classify known and unknown threats in complex mixtures – especially those that, today, are known to result in false-alarm rates so high that other sensors are effectively useless.

Turning from sensors to making sense of information, our Bio-ALIRT (Bio-Event Advanced Leading Indicator Recognition Technology) program, one of our IAO Programs, is developing software to detect covert biological attacks early through statistical, population-level analysis on

items like school and work absences, over-the-counter medicine purchases, nurse hot line and poison control center calls, and even animal illness.

Because the surveillance target of Bio-ALIRT is diseases and not people, individual identifying information is not needed or wanted. What is important is statistics about the population, not the activities of any individual. We are also using medical information in nontraditional ways, examining items such as initial complaints or tests that are ordered, rather than waiting for formal diagnoses. Advancing the time we detect an attack by even a few days could help cut short an epidemic and prevent as many as half the casualties.

Bio-ALIRT technology is currently being used to monitor the health of our nondeployed military forces world-wide and will soon be incorporated into the Joint Medical Workstation for use by Central Command's command surgeon and his staff. Bio-ALIRT technology is being tested and evaluated around Washington, DC and Hampton Roads, Virginia, which have large concentrations of military assets.

Software developed at the University of Pittsburgh and Carnegie-Mellon University has been made available to public health departments for their use. In fact, Bio-ALIRT technology identified outbreaks of scarlet fever around Washington and the Norwalk virus at the Marine Base in San Diego, before they were noticed by local public health authorities.

#### **Minutes to Hours after an Attack**

In the minutes to hours after a biological attack, we need to protect the people in the area of the attack. Our most prominent program addressing this time period is the Immune Building program, the goal of which is to keep people safe inside a building that has been attacked by bioterrorists. The Immune Building program predates the anthrax attack on the Congress, which demonstrated why such an effort is needed. Protecting a building from an outside attack, while not trivial, is fairly well understood. The more insidious attacks originate inside a building, as the anthrax letters of 2001 demonstrated. Unfortunately, the Heating, Ventilation and Cooling (HVAC) systems in most office buildings actually spread an agent around the building and infect even more people. DARPA is developing components, systems, and architectures so "smart" HVAC systems, including sensors and neutralization devices, could be used to protect the

occupants of the building from attack and isolate the attacked area, instead of exacerbating its severity. These systems are being designed to protect against chemical attacks as well.

### **Hours and Days after an Attack**

In the hours and days after a biological attack, we enter the consequence management phase, which involves managing the first responders and the medical resources to care for the victims. About two years ago, DARPA concluded its ENCOMPASS program, which was designed to effectively and efficiently deploy scarce medical resources in chaotic circumstances. A commercialized version of ENCOMPASS, LEADERS, provided medical surveillance for signs and symptoms of a biological attack for the state of New York within 24 hours of the attack on the World Trade Center. The Centers for Disease Control and Prevention (CDC) also used LEADERS to monitor for specified syndromes from hospitals in the New York City area and report them back in real-time to the CDC in Atlanta via the Internet. And, technology from ENCOMPASS is being used in emergency rooms in Northern Virginia to help 911 operators properly route patients.

In addition, while not originally designed for consequence management *per se*, other technologies that DARPA is working on today may eventually prove useful in such situations, particularly if adapted for use by first responders. For example, we are developing communications systems that could create self-forming networks for people on foot in urban environments (Small Unit Operations Situation Awareness System program). We may be able to restore communications throughout a region via a highly flexible, airborne communications switchboard (Airborne Communications Node). And our work in robotics and ducted-fan unmanned aerial vehicles (Organic Air Vehicle) could provide ways to enter and investigate attacked areas without putting more people at risk.

We must also care for the exposed victims. DARPA's most prominent medical treatment program is the Unconventional Pathogen Countermeasures (UPC) program. UPC is an aggressive and innovative program that has been trying to go far beyond "one-bug/one-drug" therapies for BW pathogens. Instead, UPC is focused on trying to develop new drugs and treatments that would be useful against all pathogens, known and unknown, naturally occurring and engineered. We are trying to make drugs to which pathogens *cannot* develop resistance. We are trying to create therapies to push out the "point of no return" – that point in the progress of



disease beyond which there is no effective treatment. Our work here is driven by the recognition that there are extremely dangerous natural threats, such as smallpox, and there are engineered threats – pathogens we have not seen before and against which our current vaccines and therapies may not be effective.

A highlight of our UPC program has been its work to eliminate anthrax as a threat, which was accelerated in the aftermath of the attack on the Congress. We have been developing six new, distinct, and complementary approaches to fighting anthrax. One is CpG, which, as I mentioned earlier, can boost immunity and the effectiveness of vaccines. Another is an extremely broad spectrum antigenomic drug that should be able to kill most pathogens. The antigenomic drug works by “jamming” DNA that has many AT pairs, the nucleic acid pair that overwhelmingly dominates the genetic code of most pathogens. Another drug is an antibiotic that works by blocking a critical enzyme that is used briefly and only during cell replication. It would be extremely difficult for a pathogen to develop resistance to either this or the antigenomic drug. A fourth compound is a protein that essentially functions as a decoy to prevent anthrax toxins from being assembled and released. This might be particularly helpful in late-stage anthrax to limit toxicity, while other drugs attack the infection. A fifth compound is similarly meant to strengthen the body’s overall resistance to septic shock, extend the point of no return, and buy time to fight the infection. The sixth program uses an enzyme called lysin as an antibacterial “precision-guided munition” that specifically targets and kills the anthrax bacterium and nothing else. Seventy percent of mice treated with this enzyme survived after they were exposed to a lethal dose of anthrax, compared to *no* survivors among the untreated mice. This approach to fighting disease was featured on the cover of *Nature* magazine last August.

I am pleased to report to you today that, based on current status of the research and assuming we continue to get good results, we anticipate that a majority of these accelerated anthrax therapeutics programs will be conducting Phase I human safety trials by the last quarter of this calendar year. This is, frankly, better than we expected. Just as important, and in keeping with the philosophy of the UPC program, most of these therapeutics show promise for many pathogens besides anthrax. For example, the antigenomic drug, when administered to mice, has shown itself to be a better treatment for malaria than the current “gold standard” antimalarial drug. And most thrilling is the fact that the antigenomic drug has shown real potential to become the first actual therapeutic for both anthrax and smallpox.

### **Days and Perhaps Years after an Attack**

Now let me turn to the last phase of the postattack timeline, decontamination. The anthrax release in the Hart Building demonstrated how difficult it is to clean up a biologically contaminated building. Even if systems such as those being developed in the Immune Building program prove successful, we must still decontaminate the affected areas of buildings.

Because of DARPA's investments in the Immune Building program, we were asked to provide science advisors to the team responsible for the anthrax decontamination of the Hart Building. We reviewed decontamination technologies and conducted quick-turnaround testing on three separate candidates to determine efficacy. The chlorine dioxide approach developed under Immune Building was selected for the challenging job of remediating the Hart Building and, more recently, the Brentwood Post Office. In addition, DARPA helped identify and obtain air sampling equipment to support the Environmental Protection Agency and CDC in verifying that the buildings were safe for reoccupation. DARPA also developed, installed, and tested mail-screening equipment to prevent additional contamination from entering the buildings through the mail system.

Finally, in the area of non-BWD decontamination, increasing attention is being paid to the threat of a radiological dispersal device, the so-called "dirty bomb." Nuclear decontamination of an area, especially an urban setting, is an enormously difficult and expensive problem and helps explain its appeal to terrorists bent on creating physical, psychological, and economic havoc. This fiscal year, DARPA has begun studying decontamination methods and technologies following an attack using this kind of terrorist device.

I hope this brief sampling has illustrated the breadth and depth of DARPA's efforts to counter weapons of mass destruction, particularly biological warfare. Our initial work in 1995 on biological warfare defense has grown and adapted, we have made very solid progress over the past eight years. But we also know the threat remains quite real and may be spreading. We continue to press ahead to develop technologies that will change our fundamental approach to all phases of the biological attack timeline.

This concludes my remarks. Thank you for this opportunity to discuss DARPA's biological warfare defense research. I would be happy to answer any questions.

FOR OFFICIAL USE ONLY  
UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE

STATEMENT OF  
DR. STEPHEN YOUNGER  
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY  
BEFORE THE  
SUBCOMMITTEE ON TERRORISM,  
UNCONVENTIONAL THREATS AND CAPABILITIES  
COMMITTEE ON ARMED SERVICES  
U.S. HOUSE OF REPRESENTATIVES  
COUNTERING THE THREAT OF WMD TERRORISM  
19 MARCH 2003

FOR OFFICIAL USE ONLY  
UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE

**Statement of Dr. Stephen Younger  
 Director, Defense Threat Reduction Agency  
 Before the Subcommittee on  
 Terrorism, Unconventional Threats and Capabilities  
 Committee on Armed Services  
 U.S. House of Representatives  
 Hearing on Countering the Threat of WMD Terrorism  
 19 March 2003**

Mr. Chairman and Members of the Committee, it is an honor for me to be here this afternoon to review the Defense Threat Reduction Agency's programs to counter the use of weapons of mass destruction (WMD). I will summarize my statement and ask that it be included in its entirety in the record

*DTRA Reduces the Threat Posed by WMD*

The mission of DTRA is simple to understand but critically important to the nation and indeed the whole world – to reduce the threat of weapons of mass destruction or "WMD." This mission has both international and domestic components, although I want to emphasize that DTRA is a combat support agency dedicated to meeting the needs of the warfighters. As a combat support agency, we exist to support the warfighters, bringing specialized expertise in the area of WMD. Where DTRA can make unique contributions to homeland security, we work through Northern Command and the Assistant Secretary of Defense for Homeland Defense and with interagency partners to make our tools and services available.

Organizationally, we report to Dr. Dale Klein, the Assistant to the Secretary of Defense (Nuclear, and Chemical, and Biological Defense Programs), but we work closely on a day-to-day basis with the Office of the Secretary of Defense (OSD), the Chairman of the Joint Chiefs of Staff, the Commanders of the Unified and Specified Commands, and the Services. To make sure that we are coupled to the needs of the warfighting Commanders, we have liaison officers assigned to the commands, allowing real-time reachback to DTRA capabilities.

*DTRA Integrates and Focuses WMD Expertise from All Sources*

When the Agency was established in 1998, it incorporated organizations with decades of experience in nuclear weapons effects, the protection of structures against high

explosives attacks, vulnerability assessments, consequence management, and arms control and cooperative threat reduction programs. This blend of expertise puts DTRA at the center of WMD threat reduction – which was precisely what was intended.

We accomplish our mission by integrating and focusing WMD expertise from all sources – the Department of Defense, other US Government entities, industry, academia, and from our allies – into products and services that meet the needs of the warfighters. Virtually every DTRA program employs a team approach involving expertise from many different organizations. Our value added is simple – we understand the need of the warfighters, find the required expertise wherever it may be, integrate that expertise into a focused response, and deliver a product within a very short period of time – often within weeks or months.

Our products range from consequence prediction to consequence management, from target analysis for warfighters to developing weapons used to be against those targets. We provide WMD expertise, technology, and support to plans and operations. We deploy our people to the battlefield to augment and support the warfighters during the pre-conflict, conflict, and post-conflict stages. For example, DTRA contributed significantly to the counter-WMD component of the CENTCOM current planning effort and we have deployed over 100 military personnel to the theater.

#### *Our Response to the WMD Threat Relies upon a Full Spectrum of Tools*

We use a full spectrum of tools to reduce the WMD threat: arms control; cooperative threat reduction; offensive and defensive technology development; defense against chemical, biological, radiological, nuclear, and high explosive weapons; and combat support. The net effect of this approach is to provide a defense in depth ranging from cooperative to non-cooperative activities that protect us both overseas and at home.

Our arms control activities allow us to take threat reduction to the source, thereby controlling potential WMD problems far away from our shores. DTRA exercises the US Government's treaty rights through intrusive arms control inspections and fulfills U.S. treaty obligations by escorting treaty partners in the US and at US installations overseas. In a related effort, in cooperation with both the FBI and the Customs Service, we are enhancing border security in the former Soviet Union to prevent WMD smuggling. Additionally, we are the DoD Executive Agent for support to the UNMOVIC inspections in Iraq.



We are also eliminating WMD threats through cooperative programs with successor states to the former Soviet Union through the Cooperative Threat Reduction program. DTRA programs provide for the elimination of strategic delivery systems, the elimination of chemical weapons, and the enhancement of Russian nuclear weapon storage and transportation security. To date, the CTR program has eliminated the delivery systems for over 6,000 strategic warheads. Furthermore, we are making progress in reducing the threats posed by former Soviet chemical and biological weapons programs. Although the execution of the CTR program has been challenging, the investment made in the program goes a long way in denying terrorists access to existing WMD.

If we cannot verify that WMD no longer exist or are being dismantled cooperatively, we develop the means to destroy or neutralize them by taking the fight to the enemy. Through its technology development programs, DTRA is the near-term interface between science and technology and the warfighter. We integrate technology from all sources – US Government agencies, the DOE National Laboratories, academia, the private sector, and from our friends and allies – into products and tools that permit the warfighter to destroy WMD stocks, WMD-related production facilities, and hardened and deeply buried targets. For example, DTRA has developed weapons that can effectively penetrate bunkers and tunnels and, using specially tailored physical effects, are designed to destroy WMD more effectively than the current inventory of weapons. We have become particularly adept at meeting unique warfighter needs with specially tailored weapons in record developmental times.

However, we must assume that, in some situations, an adversary will be successful in delivering a WMD attack against our military forces. We must be able to protect against such eventualities. We assist the combatant commanders in planning how to successfully operate through contaminated environments. We are developing an Unconventional Nuclear Warfare Defense program that will be integrated into a larger program to protect military installations against the full range of WMD threats. We also manage several related Advanced Concept Technology Development programs focused on mission execution in WMD environments. DTRA is well suited for managing the Science and Technology component of the Chemical and Biological Defense program due to our close ties to the warfighter and our ability to integrate a wide-range of expertise into focused, responsive programs.

Through our combat support programs, DTRA helps deter and destroy the WMD threat. The demand for DTRA expertise continues to grow at a tremendous rate. We assist in combat support planning and military operations, develop WMD-related concepts of operation, assess potential vulnerabilities of US facilities worldwide, support consequence management and emergency operations, and assure the viability of the nuclear deterrent. Each year, DTRA performs about 100 force protection vulnerability assessments of military installations and several dozen more extensive Balanced Survivability Assessments of key mission facilities – including, in recent years, Capitol Hill. We improve force protection and installation protection by developing technology that mitigates the blast effects of high explosives. We accomplish this through modeling and simulation, as well as field testing.

*Leveraging DTRA's Combat Support Mission for Homeland Security*

Mr. Chairman, you have heard that we are a combat support agency focused on supporting the warfighter. But I would like to comment briefly on our ability to assist homeland security. DTRA works closely with appropriate government organizations to promote the transition of our technologies for homeland security applications. For example, we are working with the Department of Homeland Security to share our experience with the Unconventional Nuclear Warfare Defense program and the Bio-Defense Initiative for American cities. We have developed WMD crisis decision guides or "playbooks" that the Department of Homeland Security has adopted as a foundation for its response plans. The creation of the US Northern Command provides the most effective means for applying DTRA support to homeland security. DTRA knows how to support such a military command and we are establishing a close relationship with Northern Command.

As you can see, we receive funding to support all of these activities not only through our own appropriated RDT&E and O&M funds, and funding for the former Soviet Union Threat Reduction, but on a reimbursable basis from other sources as well.

Mr. Chairman, this concludes my remarks. I would be pleased to respond to your questions.

STATEMENT OF  
BRIGADIER GENERAL STEPHEN V. REEVES  
PROGRAM EXECUTIVE OFFICER

FOR THE CHEMICAL AND BIOLOGICAL DEFENSE PROGRAM

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES

MARCH 19, 2003

CONCERNING

COUNTERING THE THREAT OF WEAPONS OF MASS DESTRUCTION  
TERRORISM

## TESTIMONY

Mr. Chairman and Members of the Committee. I am Brigadier General Stephen V. Reeves, the Program Executive Officer for Chemical and Biological Defense. We are located in Falls Church, Virginia. I sincerely appreciate this opportunity to represent the Department of Defense today, and to provide testimony on this important subject.

The mission of the Program Executive Office is to meet the chemical and biological defense medical and nonmedical requirements of our warfighters. The Program Executive Office for Chemical and Biological Defense executes this mission for all the armed services through the life cycle research, development, procurement and deployment of major end items of Nuclear, Biological and Chemical defense equipment as well as chemical and biological defense medical treatments, vaccines and devices. Using a focused program management structure, we maintain continuous and effective communication with the science and technology community; the Joint Requirements Office; our warfighters; industry, technical and operational testers and independent evaluators, Service logistics and sustainment activities, and with the Office of the Secretary of Defense and the Congress who have oversight responsibilities. This focused management approach ensures the rapid and effective development and fielding of new capabilities meeting joint service requirements.

In accordance with law, The Army is the executive agent for the Department of Defense's Chemical and Biological Defense Program. The acquisition professionals that lead and make up our project and product management teams come from all of the services allowing us to leverage the very best talent and technical expertise from each. Collectively, we share the goal of providing our armed forces the best chemical and biological defense medicine and equipment at the right time, at the right place, and at the right cost.

Today, I would like to show you just some of the results of the substantial Congressional support we have received since Desert Storm and the hard work by our joint service acquisition professionals. The equipment I will highlight is in use in the Gulf region today protecting our men and women from weapons of mass destruction and enabling them to accomplish their mission.

*(Equipment and Poster Display)*

In summary, we are providing our soldiers, sailors, airmen and marines the best technology, training and equipment in the world.

Again, I sincerely appreciate this opportunity to testify before the subcommittee. Subject to your questions, this concludes my testimony.

FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE

STATEMENT OF  
BRIGADIER GENERAL STEPHEN M. GOLDFEIN, U.S. AIR FORCE  
DEPUTY DIRECTOR, J-8  
JOINT WARFIGHTING CAPABILITIES ASSESSMENT  
AND  
DIRECTOR, JOINT REQUIREMENTS OFFICE  
CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR DEFENSE  
BEFORE THE  
SUBCOMMITTEE ON TERRORISM,  
UNCONVENTIONAL THREATS, AND CAPABILITIES  
COMMITTEE ON ARMED SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES  
MARCH 19, 2003

FOR OFFICIAL USE ONLY UNTIL RELEASED BY THE  
HOUSE ARMED SERVICES COMMITTEE



Mr. Chairman, the Chairman of the Joint Chiefs of Staff established a Joint Requirements Office (JRO) for Chemical, Biological, Radiological, and Nuclear (CBRN) Defense within the J-8 directorate of the Joint Staff on October 1<sup>st</sup>, 2002. The Chairman's approval included a specific charter, a manning document, and an implementation plan for the JRO. I am assigned the additional duty to serve as Director of this JRO.

The Joint Requirements Oversight Council (JROC)-approved JRO Charter calls for a single office responsible for the planning, coordination, and oversight of the joint CBRN defense requirements and to serve as the Chairman of the Joint Chiefs of Staff's single source of expertise in addressing CBRN defense issues involving the warfight, force protection, and Homeland Security. The Office's chartered responsibilities include developing and maintaining a CBRN defense Overarching Operational Concept and CBRN Defense Modernization Plan; representing the Services and combatant commanders in the requirements generation process; acting as their proponent for coordinating and integrating CBRN defense operational capabilities; developing a Department of Defense Chem-Bio Defense Program Objective Memorandum (POM), in coordination with the acquisition community; and facilitate the development of joint and multi-service doctrine.

The organizational structure calls for an office of 32 DoD and contractor personnel serving four mission areas of analysis and demonstration, mission area integration, materiel requirements, and doctrine and training development. Some of these personnel will be in joint billets and some in service billets, however they will serve as one integrated team. Each of the Services as well as the U.S. Coast Guard is contributing billets and personnel to this effort. These officers will provide initial Service input into all tasks executed by the JRO. Their presence ensures a fully integrated and joint program where the Services' concerns and equities

are heard within the requirements generation process. This is a significant change from the previous arrangement.

The JROC specifically approved the processes the JRO would use in developing the Chem-Bio Defense POM and generating requirements as follows:

First, the JRO will develop and present to the JROC for approval a prioritized list of joint capabilities. Development and prioritization of this capabilities list will depend on input from the Services and combatant commanders. Once approved by the JROC, the list will be provided to the acquisition community for developing a draft POM. Once complete, the draft POM will then be returned to the JRO for review and submission to the Secretary of the Army in his role as Executive Agent and in compliance with Public Law. The Secretary of the Army will then submit the POM to the Office of the Secretary of Defense (OSD).

Second, requirements generation will remain the duty of the Services as part of their Title 10 responsibilities, however the JRO will be responsible to ensure Service identified requirements fit into the joint warfighting operational architecture. The JRO will accomplish this by developing and maintaining the overarching joint CBRN operational concept I mentioned earlier. This concept will provide the basis for all future CBRN defense operational capabilities and be part of the over Joint Warfighting Concept. The CBRN operational concept will also provide the basis for the analysis required in developing requirements documents.

The JRO will then coordinate and facilitate integration of Service requirement into joint operational requirements through the use of Integrated Concept Teams (ICTs). Membership on these Teams will include, as a minimum, representation from the Service combat developers, and the intelligence, acquisition, and the testing and evaluation communities. Using these ICTs should ensure that all the operational requirements documents (ORDs) are fully integrated in the

development process. Once the ORD is developed, the Services will validate it and approve their respective annex. Approval of all Acquisition Category 1 ORDs rests with the JROC. The JROC delegated approval for all others to the Director, J-8.

CBRN weapons present a potentially lethal risk to soldiers, sailors, airmen, and Marines on future battlefields. It is our intent as the Joint Requirements Office for CBRN Defense to direct an aggressive program to properly identify the requirements for their protection and sustainment.

---

---

**QUESTIONS AND ANSWERS SUBMITTED FOR THE  
RECORD**

MARCH 19, 2003

---

---





## QUESTIONS SUBMITTED BY MR. LOBIONDO

Mr. LOBIONDO. As Chairman of the House Transportation Subcommittee on the Coast Guard, I remain concerned about WMD entering the U.S. through our ports. What interagency efforts are you participating in or initiating to thwart possible attacks delivered in this manner?

Dr. KLEIN. Mandated by Congress in FY02, the Defense Threat Reduction Agency's Unconventional Nuclear Warfare Defense (UNWD) Program established and continues to maintain UNWD systems at four military installations, one for each branch of the U.S. armed forces. There are UNWD systems at Kirtland Air Force Base, New Mexico; Naval Submarine Base Kings Bay, Georgia; Marine Corps Base Camp Lejeune, North Carolina; and U.S. Army Fort Leonard Wood, Missouri. UNWD systems are designed to detect, give early warning and facilitate a successful security force response to defeat an unconventional nuclear warfare attack. The UNWD system networks connect with the existing emergency response systems at the host installations. UNWD technology is not limited to radiation detectors but includes other types of sensors such as video, motion detectors, radar, and high explosive detectors. The (J)NWD networks have the capability to incorporate future improved sensors as well as chemical and biological agent sensors.

DTRA is working with the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs and the Joint Staff's Joint Requirements Office to transition the UNWD systems into DoD's Guardian Installation Protection Program. UN/VD would provide the nuclear and radiological defense portion of this chemical, biological, radiological, and nuclear (CBRN) defense program.

Two of the four UNWD systems are located at bases on the seacoast, Naval Submarine Base Kings Bay and Marine Corp Base Camp Lejeune. In addition to using UNWD sensors placed along roadways and at land vehicle portals positioned at the base gates, these installations also deploy UNWD sensors in their water approaches. At Kings Bay these included radiation detectors in buoys along the inland waterway, on various floating platforms along the marine channel into the base, and on specially equipped patrol craft. Radiation detection and identification systems to track and coordinate the interdiction of a threat approaching from the intracoastal waterway at Camp Lejeune include sensors attached to bridges monitoring the marine channel. Much of the methodology for protecting military bases from nuclear threats coming from sea are directly transferable to civilian seaports. The challenges presented by waterborne radiation detection include providing a reliable source of power to detectors, maintaining continuous communications with the land based network, and protecting equipment from the harsh marine environment.

The UNWD Program has closely coordinated with other agencies including the Department of Homeland Security to share the findings and lessons learned from the UNWD systems. The co-program managers for the Department of Homeland Security's New York-New Jersey Radiological Protection Program are especially interested in DTRA's initiatives with waterborne detection and have been thoroughly briefed on the Camp Lejeune system. Additionally, one of these co-program managers attended the public demonstration of the Kings Bay UNWD system. An independent assessment of the UNWD Program is nearing completion and DTRA plans to disseminate the findings to a broad audience.

DTRA is also an active participant along with 14 other agencies in the Department of Homeland Security's Radiological Dispersal Device/Improvised Nuclear Device (RDD/IND) Working Group. DTRA's expertise in the detection of radiological and nuclear material is especially valuable in the Science and Technology Subgroup. DTRA's UNWD experience has also been put to good use in our participation on the joint Homeland Security Council and National Security Council High Level Review Group that is conducting a review of nuclear and radiological security strategy.

Dr. TETHER. Detecting WMD that might enter our ports is an extremely difficult technical problem. The Defense Advanced Research Projects Agency (DARPA) has two small programs that could potentially address this matter. One uses gamma-ray "color" cameras that can sense both the direction and energy of gamma rays emitted by fissile materials. The other uses cosmic ray muon imaging. Both technologies build on work by the Department of Energy and its labs. We plan to inform

the Department of Homeland Security of our work so they can continue it for the U.S. port problem.

In this context, you might be interested to know that DARPA has some experience with interagency work in this general area. In the early 1990s, DARPA worked with the Customs Service to develop and demonstrate non-intrusive screening systems to detect contraband, particularly drugs, hidden in large cargo containers and vehicles using both x-rays and pulse fast neutron analysis. A partial prototype was built in Tacoma, Washington, to prove the feasibility of the x-ray to scan large containers.

Dr. YOUNGER. The Defense Threat Reduction Agency (DTRA) is involved with multiple agencies trying to reduce the threat of WMD. Protecting ports is but one small area of our broader mission. Our interactions with DHS, FBI, DOE, FAA, DOS, and ATF most often involve sharing information, conducting joint projects, and participating in joint exercises. Within the realm of Technology Development, the thrust of these interactions is to share information and technology that helps both parties better accomplish their mission.

The Contamination Avoidance at Sea/Ports of Debarkation (CASPOD) Advanced Concepts Technology Demonstration (ACTD) will examine capabilities that can be utilized prior to, during, and after an attack to mitigate the effects of a Chemical-Biological (CB) agent, toxic industrial chemical (TIC), or toxic industrial material (TIM) during the initial stages of power projection operations at sea ports of debarkation (SPOD) with limited US presence. The ACTD will develop the essential operational concepts, tactics, techniques and procedures for deployment, employment and sustainment at SPODs worldwide. The military utility of these capabilities will be assessed using 'warfighting' personnel in realistic demonstrations. Prototype capabilities used in ACTD demonstrations will be transitioned to operational units for extended user evaluations (EUE) after the successful completion of ACTD demonstrations. While the CASPOD ACTD is focused on OCONUS SPOD(s), the lessons learned may be applicable to CONUS ports. CASPOD does nothing directly to prevent the use of a WMD at a CONUS or OCONUS port, but may serve as a deterrent due to the advanced preparations the US forces will have upon arrival at a SPOD to conduct operations.

The CASPOD ACTD will address SPOD-associated challenges that result from the lack of US personnel and equipment and the absence of US-controlled infrastructure, as well as host nation issues existing at these sites.

Assumptions used for assessing the military utility of the CASPOD ACTD capabilities include the following:

- All ships arriving in port are free from CB, TIC, or TIM contamination.
- SPODs are immature and lack significant US presence (during initial stages of Time Phased Force Deployment Data (TPFDD) flow).
- Aviation ports of debarkation (APOD) operations are not considered.
- Port access is granted.
- CB mitigation efforts are primarily focused on personnel providing direct support.
- Mitigation is on a 24/7 basis, covering key workers on-and-off-duty.
- SPOD operational objectives are full ship off-load (recognizing that circumstances may exist in which only selected vehicles are off loaded. CASPOD assumes no ad hoc TPFDD adjustments after ship dispatch).
- For the purposes of the demonstrations, US military dockworkers will be used in evaluating individual protective equipment (IPE), as well as for training purposes.

The CASPOD ACTD is a five-year demonstration, which includes a three-year execution phase and a two-year residual support phase during which residuals are supported by the ACTD. During the execution phase, military utility of the CASPOD ACTD capabilities will be assessed in two demonstration events. A Preliminary Demonstration will take place at a CONUS seaport in FY03 and a Final Demonstration will be conducted in FY04 at an OCONUS SPOD. If the capabilities employed in the demonstration events are sufficiently mature, formal post-ACTD operational test and evaluation may be conducted on these capabilities to facilitate future acquisition decisions. A two-year residual support phase will follow in FY05 and FY06 for those ACTD residuals provided through the sponsoring Combatant Command. In the residual support phase, users will have the opportunity to refine operational concepts, tactics, techniques and procedures. These activities will be managed and funded by the sponsoring Combatant Command/Service Component.

Additionally, in FY02, Congress directed the Defense Threat Reduction Agency to establish the Unconventional Nuclear Warfare Defense (UNWD) Program nuclear/radiological detector systems at four military installations, one for each branch of the U.S. armed forces. There are UNWD systems at Kirtland Air Force Base, New

Mexico; Naval Submarine Base Kings Bay, Georgia; Marine Corps Base Camp Lejeune, North Carolina; and U.S. Army Fort Leonard Wood, Missouri. UNWD systems are designed to detect, give early warning and facilitate a successful security force response to defeat an unconventional nuclear warfare attack. The UNWD system networks connect with the existing emergency response systems at the host installations. UNWD technology is not limited to radiation detectors but includes other types of sensors such as video, motion detectors, radar, and high explosive detectors. The UNWD networks have the capability to incorporate future improved sensors, as well as chemical and biological agent sensors.

DTRA is working with the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs and the Joint Staff's Joint Requirements Office to transition the UNWD systems into DoD's Guardian Installation Protection Program. UNWD would provide the nuclear and radiological defense portion of this chemical, biological, radiological, and nuclear (CBRN) defense program.

Two of the four UNWD systems are located at bases on the seacoast, Naval Submarine Base Kings Bay and Marine Corp Base Camp Lejeune. In addition to using UNWD sensors placed along roadways and at land vehicle portals positioned at the base gates, these installations also deploy UNWD sensors in their water approaches. At Kings Bay these included radiation detectors in buoys along the inland waterway, on various floating platforms along the marine channel into the base, and on specially equipped patrol craft. Radiation detection and identification systems to track and coordinate the interdiction of a threat approaching from the intracoastal waterway at Camp Lejeune include sensors attached to bridges monitoring the marine channel. Much of the methodology for protecting military bases from nuclear threats coming from sea is directly transferable to civilian seaports. The challenges presented by waterborne radiation detection include providing a reliable source of power to detectors, maintaining continuous communications with the land based network, and protecting equipment from the harsh marine environment.

The UNWD Program has closely coordinated with other agencies, including the Department of Homeland Security, to share the findings and lessons learned from the UNWD systems. The co-program managers for the Department of Homeland Security's New York-New Jersey Radiological Protection Program are especially interested in DTRA's initiatives with waterborne detection and have been thoroughly briefed on the Camp Lejeune system. Additionally, one of these co-program managers attended the public demonstration of the Kings Bay UNWD system. An independent assessment of the UNWD Program is nearing completion and DTRA plans to disseminate the findings to a broad audience.

DTRA is also an active participant, along with 14 other agencies, in the Department of Homeland Security's Radiological Dispersal Device/Improvised Nuclear Device (RDD/IND) Working Group. DTRA's expertise in the detection of radiological and nuclear material is especially valuable in the Science and Technology Subgroup. DTRA's UNWD experience has been an asset in our participation on the joint Homeland Security Council and National Security Council High Level Review Group that is conducting a review of nuclear and radiological security strategy.

A related program, restoration of operations (RestOps), is an Advanced Concept Technology Demonstration (ACTD) designed to help fixed site military installations, and protect against and recover from the consequences of chemical or biological attacks. Although focused on the protection of airfields, it has some applicability to the protection of seaports. The program is divided into two phases, a three-year demonstration phase, completed in February 2003, followed by a 2-year transition phase. During the first phase, improved chemical and biological defense technologies and operational procedures were demonstrated. Units assigned to Osan Air Base, Republic of Korea, were the operational test units for the ACTD, and participated in a series of exercises, demonstrations and assessments that tested and evaluated detection, protection, decontamination, situational awareness, and selected medical technologies. These technologies do not prevent entry into the United States, but do prepare locations to handle CB incidents at fixed sites (i.e. military bases) by reducing vulnerability and quickly restoring operations.

Three major technologies that emerged from the field demonstration were the RestOps Information Management (ROIM) System, which is a computer-based system for managing base-wide situational awareness; electrochemiluminescence (ECL) tester, which is an antibody-based laboratory testing instrument that provides a faster and easier method of identifying biological agents; and the Small Shelter Patient Decontamination System (SSPDS), which supports medical decontamination operations. The U.S. Air Force has adopted the ROIM System and is currently in the process of fielding this system at overseas bases.

General REEVES. The Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) is the acquisition executive for the Department of Defense



(DoD) Chemical and Biological Defense Program (CBDP). We are primarily responsible for developing and acquiring chemical and biological agent detection, protective, and decontamination equipment and medicines for the DoD.

The JPEO-CBD procured detection and protective equipment and vaccines that have been furnished to non-DoD agencies with missions that may involve port protection including the Federal Bureau of Investigation, Secret Service, Department of Health and Human Services Centers for Disease Control and Prevention, and the Coast Guard. We have undertaken discussions with the Coast Guard to determine their chemical and biological defense requirements and how our future system acquisition plans might support their efforts.

The JPEO-CBD participates in several chemical and biological defense inter-agency groups such as the Inter-Agency Board for Equipment Standardization and Interoperability, the President's Subcommittee on WMD, and Department of Homeland Security working groups. We also participate in symposia with the National Science Foundation, Department of Homeland Security, and Department of Agriculture to provide a comprehensive review of chemical and biological detection technologies research and development efforts for industry.

In addition, the Defense Threat Reduction Agency (DTRA), JPEO-CBD, the J-8 Joint Requirements Office for Chemical and Biological Defense, and the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs are working together to develop systems to defeat unconventional nuclear warfare attacks. Management of the Unconventional Nuclear Warfare Defense (UNWD) Program is in the process of being transferred from DTRA to JPEO-CBD. The unified UNWD efforts of DoD provide critical links to several non-DoD organizations and agencies and enable the sharing of technology and expertise to combat WMD at our nation's ports.

General GOLDFEIN. The Joint Staff, J-8/Joint Requirements Office (JRO) for Chemical, Biological, Radiological, and Nuclear (CBRN) Defense requested and has been assigned a USCG liaison (O-5); he is helping to get USCG weapons of mass destruction (WMD)-CBRN requirements defined and integrated into the DOD Chem-Bio Defense Program. Through the liaison officer, the JRO is helping to shape the developing CBRN-WMD policy development ongoing at USCG Headquarters, and will assimilate the requirements and needs of the USCG in the emerging Joint Staff's FY 04-09 CBRN Modernization Plan.

# **FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT—DEFENSE SCIENCE AND TECHNOLOGY POLICY AND PROGRAMS**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ARMED SERVICES,  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

SUBCOMMITTEE,  
*Washington, DC, Thursday, March 27, 2003.*

The subcommittee met, pursuant to call, at 4:10 p.m., in room 2212, Rayburn House Office Building, Hon. Jim Saxton (chairman of the subcommittee) presiding.

## **OPENING STATEMENT OF HON. JIM SAXTON, A REPRESENTATIVE FROM NEW JERSEY, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. SAXTON. Good afternoon.

Today, the Subcommittee on Terrorism, Unconventional Threats, and Capabilities will hear testimony on the status of the Department of Defense Science and Technology Program and plans for priority and priorities for the future.

We will discuss with Director of Defense Research and Engineering Ron Sega, the military departments' science and technology chiefs, and the Director, Defense Advanced Research Projects Agency (DARPA), some of the issues faced by the program today, how the program has been reshaped to support the war on terrorism and support to our forces in Iraq and what needs to be done to accelerate the identification, development, and transition of advanced technologies we will need to ensure superiority of our armed forces on the 21st-Century battlefield.

In 1983, then Secretary of Defense Caspar Weinberger said, quote, "We face the danger of losing our edge because we have not adequately replenished the reservoir of scientific concepts and knowledge to nourish future technologies during subsequent years of fiscal neglect in defense research and development.

"Given these circumstances, we must systematically replenish the scientific reservoir, using the unique and diverse strength of the United States scientific community. Given the relatively long lead time between fundamental discovery and applying such knowledge to defense systems, the true measure of our success may not be apparent for several decades. When the moment of truth arrives, we cannot afford to be found wanting."

Secretary Weinberger was very wise in his statement.

Technological superiority over our adversaries is a cornerstone to the U.S. national military strategy. Historically, a robust Defense Science and Technology Program has been key to meeting the



known needs for military capabilities, providing a technology bridge to new weapons systems during periods of reduced funding for development and acquisition, and enabling the development of totally new operational concepts and capabilities.

The combat capabilities that overwhelmed the Iraqi army in Operation Desert Storm in 1991 were the result of technology investments made in the 1950's and 1960's. That matured into development and acquisition programs in the 1970's and 1980's. Advances in semiconductor technology and information technology in the 1970's and 1980's are the heart of the weapons systems and command and control that are the focus of the precision-strike capabilities being used in Iraq this very today.

Basic and applied research in areas such as nanotechnologies, robotics, wide band-gap semiconductors, and the biological revolution will lead to further radar and weapons systems in the future and to other capabilities for our armed forces that are yet to be—that are as yet unforeseen.

For the past two decades, both before and after the end of the Cold War, previous administrations and the Congress have faced the issues raised in Secretary Weinberger's 1983 statement regarding the Defense Science and Technology Program. These issues confront the Bush administration and the Congress as of today.

And let's just look at a few of them. There are a number of questions that, I think, are extremely important.

For example, what should the role of the Federal Government and the Department of Defense (DOD) be in supporting science and technology research and development?

Or, on what technologies should Defense science and technology (S&T) Program focus?

Next, what is the appropriate level for funding for the program?

In addition, how do we plan to manage the program more effectively and efficiently?

Moving along, what is the relevance of Department of Defense laboratories to the program, and what are—what is needed to support the aging laboratory infrastructure?

In addition, how do we ensure a continuing supply of competent engineers and scientists for defense research and acquisition, and how do we accelerate the transition of technology from the laboratory to the military user in the field?

And finally, how are we changing the programs to support the war on terrorism and the other threats that confront our nation?

Our witnesses today are the honorable Ronald M. Sega, director of Defense Research and Engineering; Dr. A. Michael Andrews, Deputy Assistant Secretary of the Army for Research and Technology; Rear Admiral Jay M. Cohen, Chief of Naval Research; Mr. James B. Engle, Deputy Secretary of the Air Force, Science and Technology and Engineering; Dr. Anthony Tether, Director of DARPA.

Gentlemen, we welcome you here today. You are familiar faces, and we welcome you back, and we are anxious to hear your testimony.

And, Dr. Sega, before we begin, I would like to yield to Mr. Jim Turner for any statement that he may have.

[The prepared statement of Mr. Saxton can be found in the Appendix on page 217.]

# STATEMENT OF HON. JIM TURNER, A REPRESENTATIVE FROM TEXAS

Mr. TURNER. Thank you, Mr. Chairman.

I join you in welcoming our witnesses today. I am standing in today for our ranking member of this subcommittee, Congressman Meehan, was unable to be with us because of a previously scheduled commitment. But it is an honor to be back in this chair that I occupied with the chairman in the last Congress on the terrorism panel.

There is certainly no more important issue than the one we are discussing today. That is the effort to effectively modernize and transform our forces to meet the threats that we find on the battlefield of the 21st Century, and I join the chairman in commending each of our witnesses that are here today for the outstanding leadership that you provide to us in achieving that objective.

I share some of Chairman Saxton's concerns about the administration's budget request in this particular area, and I have a few of my own concerns.

First, the totality of the Navy science and technology investments are once again, in my judgment, unsatisfactory and fall well below the Department's stated goal of 3 percent of total Research and Development (R&D) funding.

I also note the Army's priorities seem overly dependent upon what I perceive to be a risky and perhaps unrealistic investment strategy aimed at fielding the Future Combat System by 2008.

And finally, I would note that the department's request to migrate programs from the Office of the Secretary of Defense (OSD) to the service is another concern that I have. Many of these programs that were placed with OSD to promote the development of joint capabilities, in my judgment, cannot be achieved by devolving them to the services. These changes, in my judgment, are a step backwards.

And I hope that the witnesses today will address each of those concerns that I have and share with me your thoughts and views on them.

Our goal here, of course, is to provide the best military capability possible in the most cost-effective manner that we can.

In addition to addressing the issues I mentioned, I hope that each of our witnesses will share with us some examples of how your developed capabilities are currently being utilized to degrade the enemy in Iraq. We have heard news reports of some of those capabilities, and those that can be shared in an unclassified setting, I hope you will do so.

Mr. Chairman, I join with you in your commitment that you have exhibited throughout the years in ensuring that we are prepared to meet the threat of terrorism. I am pleased that you are the chairman of this committee because your entire career in Congress has been devoted to addressing the threat of terrorism, a threat that you noted way before most of us did.

Mr. Chairman, with that, I thank you for the opportunity to be a part of this panel review today.

Mr. SAXTON. Thank you, Jim.

As the chairman of the full committee would say, we are going to fire away now, and we are going to start with the Honorable Ron Segal.

**STATEMENT OF HON. RONALD SEGA, DIRECTOR, DEFENSE RESEARCH AND ENGINEERING, DEPARTMENT OF DEFENSE**

Dr. SEGA. Thank you, Mr. Chairman.

Members of the committee, thank you for the opportunity to appear before you today to talk about transformation and the Science and Technology program of the Department of Defense.

I request that my formal statement be submitted for the record.

Mr. SAXTON. Without objection.

Dr. SEGA. As the director of Defense Research and Engineering, functioning in the roll of the department's chief technology officer, I have established five goals: Integrate the DOD's Science and Technology Program and focus on transformation; enhance technology transition; address the national security science and engineering workforce; expand outreach to the combatant commanders and intelligence community; and, number five, accelerate support for the war on terrorism.

The Department of Defense has requested for science and technology in the fiscal year 2004 budget request approximately \$10.2 billion, or 2.69 percent, of the overall DOD request. While this is a sizable investment and an increase over previous years, it falls short of Secretary Rumsfeld's stated goal of having science and technology investment be about three percent of the total DOD budget.

The first goal is that of integrating DOD's S&T and focus on transformation. It is our goal—and we have done this in a collective way, the sciences—services and agencies—to provide an integrated approach to the Science and Technology (S&T) Program in the department.

We have established a process of looking at the goals established by the secretary, the Quadrennial Defense Review goals, and assessing how we have done in terms of our investment across department with the services' and agencies' investments.

We also have in place processes of looking at the individual investments on a technology level to see if there is unwanted redundancy. Some are desired. Others are not. But we have a formal process that is in place to examine technology across the Department of Defense.

In addition to the various services' and agencies' focus areas, I would also like to highlight three areas that are cost cutting.

One of those is National Aerospace Initiative, which includes high-speed hypersonics research, access to space, and space technologies.

In the fiscal year 2004 budget request, the department focused an increased investment in hypersonic technology, investing over \$150-million additional funds in hypersonics. It has an application to various missions and participation by all the services.

We seek congressional support for the fiscal year 2004 budget request for the increased hypersonics work and the integrated tech-

nologies of space access and space technologies of the National Aerospace Initiative.

The second cost-cutting area is in the area of energy and power technologies, one that is enabling an electric force of the future, includes technologies in the areas of power generation, whether it be from diesels, jet engines, fuel cells, and so forth; energy storage, whether it be in batteries, capacitors, energetic materials; conversion of that energy, which is in switches; and a special emphasis on directed energy.

The third cost-cutting area is in the area of surveillance and knowledge systems. Here, we are looking at an emphasis on sensors and robotics, special emphasis on chem-bio-nuclear sensors, high-bandwidth communications, information assurance, information and knowledge management systems, and a special emphasis on cyberterrorism.

The second major goal is enhancing technology transition. The department is streamlining the acquisition process built around spiral development and evolutionary acquisition. So, to enhance this technology transition, we need means and incentives to programs to also accept the new technology.

The department is implementing three pilot projects contained in the Quick Reaction Special Projects (QRSP) Program that was funded in fiscal year 2003 at \$25 million. The three QRSP projects are complementary in focusing on developing technologies at different maturity levels.

At the very early stages, the idea stages, the Quick Reaction Fund. Later on, as the technology is kind of demonstrated, the technology transition program and technology transition initiative. And third is the Defense Acquisition Challenge Program for more mature technologies that can be inserted in programs of record.

In the fiscal year 2002 appropriations bill for the Defense Emergency Relief Fund, Congress identified \$15 million for Quick Reaction Munitions Funds. This is the type of work we expect in a Quick Reaction Special Projects Fund as well.

The two areas that we accelerated were Thermobaric Hellfire Enhanced Capability, and we went from chemistry to the field—and I will speak more about that later—in roughly 12 months at a cost of \$13 million.

The second project was Low Cost Guided Imaging Rocket, and that is the enhancement of unguided 2.75-inch Hydra Rockets used in close air-to-ground operations. An interesting development there was taking technology from the nightvision laboratory in government, transitioning it actually into the automotive industry where we then picked up the technology once again and applied it in a more low-cost way to this problem of guiding a 2.75-inch rocket.

We believe the payoffs for the QRSP Program are very high, and we have consequently added \$50 million to the fiscal year 2004 budget request compared to fiscal year 2003. So we seek Congress's approval and support for the program at the level of \$75 million in fiscal year 2004.

It will ensure us that we have another tool for the flexibility that we need for execution of your programs. New needs arise from the field, and technologies are revolving at a very rapid rate, and this enables us to react rapidly.



The third area is addressing the national security science and engineering workforce. This is important to assure innovation in DOD areas into the future. It is a broad national strategic issue involving the availability of scientists and engineers in the United States and particularly in certain areas of interest to the Department of Defense that are American citizens.

The fourth area is expanding outreach to combatant commander and the intelligence community for enhancing the connectivity between the combatant commands and the intelligence community so that we would be better aligned with our S&T investment to the needs of the warfighter.

The fifth area is to accelerate support for the war on terrorism. We believe this is our most important near-term goal. In September of 2001, we established a Combating Terrorism Technology Task Force in the Department of Defense. That was on September 19.

On the 21st, some 150 technology candidates were brought forward by the services and agencies that could potentially be fielded in a month or so down the road. We accelerated three of those at that time.

One was a talcum penetrator, a second was a Nuclear Quadrupole Resonance System, and the third was a Thermobaric explosive. In 90 days, we went from chemistry of the Thermobaric mix, which was being done at Indian Head, by the Navy, and a chemistry state during the month of October, selecting a leading candidate, tested it in static conditions in the Nevada site in November, flight-tested it November, and certified it as a fielded system within 90 days of starting. That is one example.

As we move forward into this year, the fiscal year 2002 Quick Reaction Munitions Funds, as I mentioned, for an extension of that quick technology development in the Thermobaric explosives—we have adapted over the last roughly 12 months to accommodate the system of a Hellfire Missile. So we have taken that knowledge, that S&T investment, and enhanced it and applied it to another system.

In this case, the Marine Corps led that with partners of DTRA and the Army. The previous work had been done with the Navy, DTRA, the Air Force, and the Department of Energy. So there are examples of meeting warfighter needs, use of money that was available in the near term, and involving multiple services and agencies to bring a capability to bear for the warfighter.

In closing, this S&T Program and the objectives of Secretary Rumsfeld to provide transformational capabilities to DOD are absolutely intertwined. I have mentioned only a few examples within the DOD S&T Program. I believe the Department of Defense successes in technology and transformation are significant, and I appreciate the opportunity to come before you today and tell you about them.

Thank you for your continued support for S&T and DOD.

[The prepared statement of Mr. Sega can be found in the Appendix on page 219.]

Mr. SAXTON. Ron, thank you very much.

We will turn now to Dr. Michael Andrews. As I said, he is Deputy Assistant Secretary of the Army for Research and Technology. Dr. Andrews.



**STATEMENT OF DR. A. MICHAEL ANDREWS II, DEPUTY ASSISTANT SECRETARY OF THE ARMY FOR RESEARCH AND TECHNOLOGY**

Dr. ANDREWS. Thank you, sir.

Chairman Saxton and members of the subcommittee, I want to thank you for this opportunity to discuss how the Army's Science and Technology Program is pursuing solutions that will maintain the momentum of the Army's transformation. I previously submitted by written statement and request that you accept—

Mr. SAXTON. Dr. Andrews, could you pull that mike over a little bit closer to you there?

Dr. ANDREWS. I am sorry. It is one of these three.

Mr. SAXTON. There you go. Now you have got two.

Dr. ANDREWS. Sorry about that.

I have previously submitted a written statement and request that it be accepted for the record.

Your Army Science and Technology Program is dedicated to providing our soldiers with the technology for decisive victories today and tomorrow. Just six months ago in Afghanistan, a key technology, Interceptor Body Armor, saved soldiers' lives in Operation Anaconda. That came from our Army labs.

Today in Iraq, fighting in Iraq, we have Abrams and Bradley fighting vehicles, combat vehicles, equipped with second-generation nightvision technology, TV quality, longer range, greater identification capability. We also now have a man-portable anti-tank missile called Javelin that is out there, was not there in Desert Storm.

So our soldiers, your gallant soldiers, are on point for America, and, as we talk in the Army about the see first, understand first, act first, and finish decisively, we are all about the support to that.

This is our fourth year of Army transformation. In 2000, we established a memorandum of agreement with DARPA for the Future Combat Systems (FCS). This is the number one Science and Technology Program for the Army. It has become a joint requirement also.

In 2002, DARPA and the Army awarded FCS Lead Systems Integrator contractor to the Boeing team. This year, in 2003, we are seeking Department of Defense's approval to proceed in the systems development and demonstration. That is transformation in action.

I would like to show you now a four-minute video, which captures much of the progress that has been made between ourselves and DARPA. When I last testified before this committee two years ago, the technology I showed you then was primarily depicted as ideas, concepts, and artwork.

If I could play the video—it is about four minutes. I will stop it about three times to show you. This is our technology that has been in progress Future Combat Systems.

Roll it.

What you are going to see is the power of FCS immersed in an integrated environment with the force of the network. We have taken a little bit of animation but lots of hardware being demonstrated in the field.

What you see here is we have been called into action somewhere. We are taken to where we need to go by the Air Force. We count

on the Navy to help us where we need to be. And then, at the end of the day, we are on the ground somewhere.

And, very importantly, when we are on the ground, we do not have time stop, set up an operations center. We are going to have to be able to get there and communicate for reachback, communicate where the Joint Forces—the other forces may be.

Importantly, we have now demonstrated we can do satellite communication on the move, up to 40 miles an hour off road. Inside that vehicle—If you play it, please, again—Inside that vehicle is four stations with a collaborative station. What we have brought in place here is an ability to show collaboration on the move. A key part of the Future Combat Systems is a significant fraction will be unmanned, air and ground, and the ground is the most tough—one of the more difficult challenges. You have terrain, and you have issues of getting beyond the trees that may be in there.

So let me show you in the next piece as we roll how we have attacked this in two parts: autonomy, get through the woods on your own, from Point A to Point B. This is no man in the loop. You are told to go from Point A to Point B.

Now we are out in the desert. Fort Bliss three weeks ago. You park the vehicle across the road. It knows to go around it, and it knows to stay on the road, very importantly, because that other side of the road might be—have something else there.

We also attack mobility, build a vehicle that can just about follow you anywhere. This is a six-ton vehicle getting at the ability to transport parts and people.

The next part is a—what we might call a mule, and this is getting at being able to transport possibly 350 pounds, and, when it comes across a problem, it figures out how to solve that problem rolling its tires around, as you see.

Now one of the harder parts to visualize about Future Combat Systems is the network because the network is transparent to this obviously. But, importantly, you talk about the key words of scalable, ad hoc, healing.

As the vehicles move through a terrain—and they can only have line of sight—we are going to count on unmanned air vehicles to give us the relays, give us the eyes in the sky, and we are going to have to interact with manned vehicles, such as the Black Hawk you see here.

Up at Fort Dix, we have been demonstrating for the past three months—

Mr. SAXTON. That is a good place.

Dr. ANDREWS. Yes, sir. [Laughter.]

Dr. ANDREWS. It is a great National Guard facility.

Mr. SAXTON. You did not do that on purpose, did you?

Dr. ANDREWS. What we hope to do is replace some of these surrogate vehicles with unmanned aircraft. What you see demonstrated here is about a 6,000-pound helicopter, totally unmanned, no man in the loop, no one flying it, go out, Point A, Point B. Ultimately, it will carry about 200 pounds 40 hours.

Now a key part is demonstrating on the move and can we do it with quality of service. What you see running across Fort Dix there is the ability to manage the network, make sure the high-priority messages get to the right people in the right time.

Now, as we move to finishing decisively, let's say, and acting first, it is about making sure we put down trip wires wherever the enemy may penetrate and making sure that if we—if the enemy does cross those lines essentially that are connected by the electrons that we send out a signal.

And here, we have seen a vehicle coming down the road. We sent the signal up to Multi-Sensor Acquisition and Targeting (MSAT), got a picture, put it back inside the cabin, inside the manned vehicle. Now we are flying some small unmanned aerial vehicles (UAVs) out to get it. In a few minutes, you are going to see DARPA's nine-inch version of this that went and flew and were coupled well at the hip.

Another part is now, as you are in the move, you want to call for fire, and one of the key parts of this program is a precision attack missile. It is in a box being launched. There are four-by-four in there, with one piece of it for command and control. It goes out about 19,000 feet up, about eight clicks out, will ultimately get to 40 kilometers.

We also test-fired at Fort Dix a Javelin on a tele-operated vehicle.

We demonstrate we can build 20-ton vehicles fitting inside C-130.

Now let me just stop for a moment on this one. We are at 20 tons. There are risks there when you are at 20 tons. Abrams is 70 tons. Thirty-five tons of it is armor. There is a reason for that. If you do not have those extra 35 tons and you are under 20, you need some other kind of protection system. The situation awareness, the network is part of that.

What you see here on the upper right is the target. Where the target is sitting in the upper left, two missiles are launched nearly simultaneously coming in as—they are both taken down. One by electronic warfare. One by munition.

Roll it.

You see the launcher came up there. The missile is going to go and bite the dust in the top one. The next one, the launcher sends out a munition of ball bearings and essentially destroys the incoming round. So the potential of not getting hit is beginning to be there for capability for Future Combat Systems.

At the end of the day, it is about finishing decisively with soldiers somewhere, and they have got to be able to communicate. They have got to be trained well. So you go in with the best training that you could have before you get there.

We just had a demonstration as part of the overall effort of something called the situational understand—situational—small-unit operation situational awareness system, DARPA design. We are building this next version that takes it down to soldier size.

So that is the power of Future Combat Systems. That is the progress that has been made.

Let me finish a little bit of my testimony then.

I want to highlight three other Objective Force S&T pieces for 2004: the Objective Force Warrior Program, the Unmanned Combat Armed Rotorcraft collaboration with DARPA, and our efforts to pursue paradigm-shifting technologies through our Basic Research Program.

The Objective Force Warrior Program applies a system-to-system approach for the individual soldier. This is a \$240-million effort over the fight. It takes network, lethality, and survivability developed for the Future Combat Systems directly to the individual soldier.

We will provide the soldier with the full capabilities of the network, while reducing today's almost 90-plus-pounds of combat load down to 40 pounds and in three years.

Our single largest aviation Science and Technology Program is the Unmanned Combat Armed Rotorcraft partnership with DARPA established in 2002. This is a \$500-million cost-shared effort. Here, we are demonstrating the war-fighting payoff of an Unmanned Armed Rotorcraft as a complement to manned systems.

Finally, let me discuss our broad and diverse Basic Research Program. Here, we draw upon the best and brightest of American academia to focus on Army needs for our soldiers. The foundation of Army basic research rests on our single investigator's program.

But we have also established university, industry, and Army partnerships to create what I call critical mass and paradigm-shifting technologies. The first two of these are an immersive—what we call immersive environments where you place soldiers in an environment for the best possible training.

So next in nanosecond technology. This is about getting soldiers survivability, ballistic protection in a uniform.

This year, we established a third paradigm-shifting partnership. This is in biotechnology, by—to new sensors for mine detection possibly.

Now, of course, only with top-caliber scientists and engineers who develop the technologies for our soldiers can we achieve the transformational goals for Future Combat Systems and Objective Force. Recruiting and retaining these important members of the innovation team is a challenge across DOD. Our soldiers depend on these people.

In closing, the Army S&T community has stepped up to the technical challenges necessary to enable the Army's transformation. We have energized all of our resources and are committed to making the Objective Force a reality. Your contingent support is essential for this Army transformation.

Thank you.

[The prepared statement of Dr. Andrews can be found in the Appendix on page 250.]

Mr. SAXTON. Thank you, Mike.

We are going to move now to the chief of Naval research, Rear Admiral Jay Cohen.

#### **STATEMENT OF REAR ADM. JAY COHEN, CHIEF OF NAVAL RESEARCH, DEPARTMENT OF THE NAVY**

Admiral COHEN. Mr. Chairman and members, I must tell you that I am honored and humbled to testify before you today. I am joined behind me by the Officer of Naval Research Vice Chief of Naval Research Brigadier General Frank Panter, a Marine combat engineer.

Mr. Chairman, I have provided a written statement, and I ask that it be entered into the record. I do not intend to read it.



Mr. SAXTON. Thank you.

Without objection.

Admiral COHEN. This great nation is at war today halfway around the world in a fight to free Iraq, to defeat the despicable agents of terrorism.

When we are victorious—and we will be victorious—the speed of that campaign and any American and coalition fighter lives saved, as well as the lives of non-combatants, I believe, will be the result of the sustained and generous investment that the Congress has made in science and technology that has given the United States unprecedented asymmetric advantage to win.

And so, on behalf of the Department of the Navy Sailors and Marines and their families, I thank you for that.

With deference to the tasking that we have received during your initial comments, sir, I just wanted to follow-up a little bit on Dr. Sega's comments on the Counterterrorism Technology Task Force, of the three items he mentioned, that two of those were Naval in their basis.

One was the Thermobarics. That was the 60-day wonder, the cave buster, that was 30 years in development. It started with the USS *Forestal* fire, which was tragic, and it was an attempt by the Navy to find more stable explosives which resulted in much more powerful explosives. So the 60-day wonder that took 30 years to sustain science and technology.

The Nuclear Quadrupole Resonance detector efforts at the Naval Research Laboratory to determine how they might detect plastic explosives which are high in nitrogen molecules, understanding how the nitrogen molecule or atom responded in a quadrupole resonance manner gave us the ability to have the equivalent of the screener that you have when you go to the airport for your baggage.

And probably most impressive, in 1992, the Naval Research Laboratory was awarded the Collier for its efforts in developing the Global Positioning System (GPS). That came out of a \$75,000 investment that was hotly contested within Naval Research in the mid 1970's to determine the more precise measurement of time by orders of magnitude that gives us the accuracy that we enjoy today, and, at that time, that researcher had no idea of the multibillion-dollar industry and the capabilities that that small investment would give.

Dr. Sega said that we are going electric. I am pleased to tell you that recently we have started the construction of the Electromagnetic Air Launch System. We have parallel risk-reduction efforts, both in General Atomics and Northrup Grumman, at Lakehurst in New Jersey, but it is not just about launching aircraft on the new CBN-21.

We want to do away with steam, air, and hydraulic auxiliaries. You have to provide the power. And we recently went to contract with American Superconducting up at Fort Devens for a 36-1/2-megawatt. That is 50,000 shaft horsepower, 120 RPM, direct-drive motor that will be available in 37 months that will go on DDX or on the X-Radford for risk reduction on our first all-electric ship, and, together, those will be used to enhance electric weapons, which we see changing naval warfare.



I notice Jefferson Laboratories are represented here where we are working with them on free-electron lasers which, we believe, within three years, will demonstrate weapons-grade lethality.

Finally, I just want to talk about a million dollars that as chief of Naval Research—I am in my third year—I think was the best spent of any monies that I have spent so far, to revitalize our precious S&T workforce. And it is graying. The median age now is in the 50's, which does not sound too old to me, but it is something that takes attention.

A year and a half ago, through our Naval Reserve Hoster training units around the country, we offered summer stipends on the order of \$3,000 to \$4,000 for rising juniors and seniors in college and post-graduate students to select the Naval Research Laboratory or warfare centers all around the country to be summer interns for a period of eight to 10 weeks and work side by side with our government scientists and engineers.

We had on short notice 830 applicants, 163 participated. I got to talk with almost all of them because we set a very broad net across our Naval Reserve Officer Training Corps (NROTC) units all around the country. I can tell you when you look at the pictures, you see the face of America everywhere.

This year, we have increased the number. We already have 1,800 applicants, and we anticipated a modest increase in the program, that over 260 will go to our laboratories and warfare centers.

And the most exciting thing—

And they were mentored, taken home, provided food and shelter.

The most exciting thing is the majority of them want to come back, and those that are graduating are starting to apply to be government scientists and engineers.

So we thank you for your support, and I look forward to answering your questions, sir.

[The prepared statement of Admiral Cohen can be found in the Appendix on page 260.]

Mr. SAXTON. Thank you very much, Admiral.

We are now going to move and hear from the Air Force.

Mr. James Engle.

#### **STATEMENT OF JAMES ENGLE, DEPUTY ASSISTANT SECRETARY OF THE AIR FORCE (SCIENCE, TECHNOLOGY AND ENGINEERING)**

Mr. ENGLE. Thank you, Mr. Chairman.

Members of the subcommittee and staff, I very much appreciate the opportunity to provide testimony—

Thanks, Mike.

To provide—on our program—fiscal year 2004 Science and Technology Program.

The United States Air Force is transforming to the capability-focused Expeditionary Air and Space Force, as I am sure you are aware.

We have taken the effects and capabilities required by our Air Force concepts of operations and mapped them to our long-term challenges and short-term objectives identified in the congressionally mandated S&T planning review completed in February 2002.

Our goal is to make the warfighting effects and capabilities we need—and the capabilities we need to achieve them the drivers for everything we do. This is especially true on our S&T program.

The United States Air Force is committed to a robust S&T Program that enables us to achieve our vision of becoming an integrated air and space force capable of rapid and decisive global engagement.

Transforming our warfighting capabilities toward this end will involve continuous innovation in how we think about employing our forces to defend our nation, as well as quantum leaps in our technology.

We must be prepared to counter regional instabilities, the worldwide availability of advanced weapons, and other emerging and less predictable asymmetrical threats.

We are developing transformational technologies that permit flexible forces to operate far from home, on short notice, for extended time periods.

However, we must also be able to afford these innovations, once we develop them, in order to recapitalize the Air Force to our full vision. To meet these objectives, we search out the most promising and affordable technologies in order to win decisively, protect our forces, and minimize collateral damage.

We have been faced with the reality of a fiscally-constrained but operationally-demanding environment. The high operations tempo in the Air Force has sustained—in support of our peacekeeping operations and conflicts, such as Afghanistan, has placed a great burden on our people and our systems. In spite of these requirements, the Air Force has maintained a balanced S&T portfolio.

The Air Force fiscal year 2004 president's budget request for S&T is \$2.2 billion, an increase of more than \$535 million from the fiscal year 2003. The most significant change in this budget request results from the development of \$350 million for several Office of the Secretary of Defense efforts to the Air Force S&T Program. These include the High Performance Computing Modernization Program, a portion of the University Research Initiative, and High Energy Laser Joint Technology Program.

As the Air Force understands the concerns of Congress regarding the level of support for these developed programs, we are working hard to ensure execution of the programs transferred to the Air Force continues to support the diverse multiple military objectives inherent in each of these programs.

Further, the Office of the Secretary of Defense will continue to provide policy guidance and oversight for these efforts.

In conjunction with the increase in S&T funding, there has also been a significant increase in the involvement of the warfighting commands and the senior Air Force leadership in planning, programming, and prioritizing Air Force S&T.

The Secretary of the Air Force and the Air Force chief of staff, the Air Force four-stars, and other senior leaders review the S&T portfolio on a routine basis. The latest senior leadership review focused on transformational technologies that can be developed to assist in combating terrorism and other asymmetrical threats.

The Air Force scientist and engineer workforce is another area where our senior leadership is involved and plays a vital, pivotal

role. Both Secretary Roche and General Jumper are deeply involved in shaping our future scientist and engineering workforce. Air Force civilian and military scientists and engineers (S&Es) are highly motivated and productive.

The Air Force is unique in that 20 percent of its laboratory S&T government workforce is active duty military. This gives us a direct link to the warfighter. Some of these military scientists and engineers come directly from operational commands, while others serve in operational commands and then later in their careers serve in S&T.

The Air Force is committed to shaping its S&E workforce with the vision to enhance excellence and relevance of science and technology into the 21st Century and appreciates the support Congress has already provided. We, as others do, find it difficult to recruit and retain S&Es. However, the Air Force has several initiatives, both military and civilian, that address recruitment and retention issues.

We are employing the Airman's Education and Commissioning Program and the Technical Degree Sponsorship Program to recruit additional scientists and engineers into the military workforce and bonus programs to shrink the current shortfall in our military scientists and engineers.

On the civilian side, the Air Force Laboratory Demonstration Project has provided the Air Force Research Laboratory with some key flexibilities needed to compete with private industry for critical science and engineering talent. These flexibilities will need to be considered as a national security personnel system is developed.

Initiatives such as the special hiring legislation authorized by Congress in Public Law 106398 which provides DARPA-like hiring authority to the military departments should also produce positive results in shaping our S&E workforce. This authority has only recently been delegated to the Air Force, but we are optimistic about its potential, and, again, we express our thanks to Congress for your continued support.

As technical superiority is increasingly a perishable commodity, we work hard to optimize our S&T funding, not only by inventing the future ourselves, but also speeding the introduction of new technologies to our warfighters. One way of rapidly transitioning technology to the warfighter is through our Applied Technology Councils and Advanced Technology Demonstrations.

The Applied Technology Councils were initiated in fiscal year 1999 to foster top-level user involvement in the transition of technology from laboratories to the system developer to the operational user.

The Councils are composed of two-and three-star generals from the Air Force Research Laboratory, our logistics centers, our acquisition product centers, and our major unit user commanders to formally prioritize the Advanced Technology Demonstrations.

We hold Applied Technology Council meetings with each major command twice every year and have commissioned 34 Advanced Technology Demonstrations that have transitioned funding. This process facilitates technology transition to operational use and secures user commitment for resources to do systems design and development and fielding of technology.

While traditional focus on S&T has been on developing long-term capabilities, the Air Force S&T program also contributes to current needs for the Nation and our troops deployed in hostile areas.

One example of the Air Force—of an Air Force project receiving a great deal of attention since September 11 is the Elastomeric Coating polymer, which was developed by the Air Force to protect key buildings and installations from close proximity explosion, such as air-dropped weapons or truck bombs.

This easy-to-apply spray coating provides greater structural integrity of external walls and prevents dispersion of debris as well as separation of wall elements. In addition to protecting lightweight shelters, this polymeric coating is currently being applied to the interior of the outer walls of the Pentagon.

Another transformational effort is the Vehicular Mounted Active Denial System, or VMADS. VMADS is a currently developed—jointly developed program with the U.S. Marine Corps and is a defensive millimeter-wave system used for perimeter defense application. It is a directed-energy weapon that emits a non-lethal, non-damaging beam, which heats up the skin of the potential enemy causing extreme pain and forcing the person to flee.

They have a demonstration of this technology at full weapons parameters on volunteers at a range beyond that of small arms. I have brought along a small demonstration model, which we call a finger zapper, if any of you would like to test it, and I think we have it over here.

And it is quite impressive. If you have some time after the hearing, I would certainly urge you to give it a try. I guarantee you that it will not hurt you, but it will certainly demonstrate what the sensitivity of a human being would be if involved in the full beam of this weapon.

In the war on terror, Special Tactics Controllers—and I would be happy to test it first for you just to let you know that, or I am sure Mike would. [Laughter.]

In the war on terror, the Air Force Special Tactics Controllers are changing the very nature of warfare. By performing operations deep in enemy territory, they help determine who the terrorists are, where their weapons are located, and who the innocent civilians are.

Then they precisely control the elements of air power to defeat the terrorist threat, while taking care to spare the innocent civilians and minimize collateral damage. Then these Special Tactics Combat Controllers are there to provide instant battle-damage assessment.

We call these deep engagements Battlefield Air Operations (BAO).

To give you an idea of what these Special Tactics Warriors carry with them, I have brought a sample of the pack with me, and I think we have that somewhere around here, and—I would go and pick that up for you, but I think it is probably beyond my capacity. It weighs about 150 pounds.

These are extremely awkward and heavy, and about half of this weight is coming from what we call the Battlefield Air Operations Kit itself. This is a collection of about 12 different individual items



that aid the Combat Controller in actually calling in fires at the appropriate time and place.

Working collaboratively with the Special Tactics Warriors, the Air Force BAO TIGER TEAM is partnered with a national team of industry participants to field significant enhancements of increasing capability while reducing the weight and size of the individual BAO Kit equipment.

These kit improvements are being realized very rapidly in spirals to speed development, prototyping, testing, production, and fielding. As a result, our Special Tactics Warriors will soon have a digital machine-to-machine capability that helps quickly connect the right aircraft with the right munition, guided precisely to the right target at the right time to achieve the desired effect.

This new automated process helps to reduce the time it takes to target the terrorist threat or other threats, while at the same time reducing human error in the targeting process. These new BAO capabilities will help save American lives and the lives of innocent civilians. The BAO provides a revolutionary and highly effective way to combat terrorist—the terrorist threat.

Another terrorist threat that is not limited to the battlefield and is growing every day is that posed by man-portable infrared air-guided systems. These ubiquitous missiles threaten not only our combat aircraft but our large transport aircraft, both military and civilian.

To counter this menace, the Air Force is developing and testing the technology for generation on-board directed-laser infrared countermeasures, an effort focused on providing self-protection for high signature platforms like the C-17 and other valuable assets.

Advanced Laser-Protected Closed-Loop Infrared Countermeasures, or CLIRCM, as we call it, multispectral missile-warning systems will enhance our capability to engage both current and future infrared surface-to-air and air-to-air missiles.

Another Air Force technology that deserves special mention is a small munition currently being flight-tested at Eglin Air Force Base, Florida, the Low Cost Autonomous Attack System, or LOCAAS, Technology Program.

This is a 100 pound flash-powered munition of which the primary target is set—set is moving and relocatable.

And I think we have one of these sitting up here. Thanks, Dan, for your inspection. This is one of the Advanced Technology Demonstration Programs I referred to earlier, and I brought along this model, as I said, that you can examine.

LOCAAS will integrate a laser-radar precision terminal seeker with an Autonomous Target Recognition algorithm, a Multi-Modal Warhead, Global Positioning System/Inertial Navigation System Mid-Course Guidance and a miniature turbine engine with a fly-out range of about a hundred miles.

This program is scheduled to complete five flight tests by the end of the fiscal year 2003, and we just completed last week its third flight test. Flying under its own power, LOCAAS acquired and identified the designated surface-to-air missile launcher target and detonated over the target at the appropriate time.

Mr. SAXTON. Is the—is the target location programmed in before takeoff? Is that what happens?



Mr. ENGLE. There is a recognition algorithm, and we can load a series of targets into the system. It uses a Laser Detection and Ranging (LADAR) sensor that identifies the target. It then correlates that with the priority set that we have loaded, and it attacks in priority order those targets.

In this particular test we did last week, we had the primary target, which was an erector launcher plus two confusing—confuser targets that were prioritized lower on the list. It actually identified a T-72 tank, bypassed that, found the erector launcher, recognized that was a higher priority, engaged that system using its LADAR identification and algorithms.

Mr. SAXTON. Pretty smart.

Mr. ENGLE. That is right.

In conclusion, the Air Force is fully committed to providing this nation with advanced air and space technologies required to meet America's national security interests around the world and to ensure we remain on the cutting edge of systems performance, flexibility, and affordability.

The technology advantage we employ today is a legacy of decades of investment in S&T. Likewise, our future warfighting capability will be substantially determined by the investments that we make today in S&T.

As we face the new millennium, our challenge is to advance technologies for an Aerospace Expeditionary Force as we continue to move aggressively into the realm of space activities.

The Air Force S&T Program provides for the discovery, development, demonstration, and timely transition of affordable, transformational technologies that keep our Air Force the best in the world.

As an integral part of the Department of Defense S&T team, we look forward to working with Congress to ensure a strong Air Force S&T Program tailored to achieve our vision of a superior air and space force.

Mr. Chairman, thank you, again, for the opportunity to present testimony, and thank you for your continuing support for the Air Force S&T Program.

[The prepared statement of Mr. Engle can be found in the Appendix on page 271.]

Mr. SAXTON. Thank you very much, Mr. Engle.

We are now going to—we are now going to go to our cleanup batter, Tony Tether, from the great agency of DARPA.

#### **STATEMENT OF DR. ANTHONY TETHER, DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECT AGENCY**

Dr. TETHER. Mr. Chairman, members of the committee, thank you for having me here today. I would like to enter my written testimony into the record.

Mr. SAXTON. Without objection.

Dr. TETHER. My written testimony and our strategic plan, which was delivered earlier this year, lays out eight major thrusts that we are working on in response to the—to potential future threats we face or new technological opportunities. These range from counterterrorism, assured use of space, robust self-forming networks, down to biology.

In addition to that, we are also continuing our work in technologies that have historically shown themselves to be powerful enablers of new defense capabilities, such as materiel, microsystems, and information technology.

I am not going to talk about these in any detail because I believe the written testimony does a good job in laying out what they are along with the strategic plan.

However, I am—I am asked many questions, as you might imagine, on DARPA, what it is, how we do what we do, and, you know, why should you—we give you more money, I guess, is—I am asked, not only here but also elsewhere. [Laughter.]

Dr. TETHER. One question I am asked is—so what I would like to do is go through some of those questions.

Mr. SAXTON. You ought to do some of those experiments up at Fort Dix. Then you would get some money.

Dr. TETHER. Well, in fact, we do. [Laughter.]

Mr. SAXTON. Well, we are getting to that.

Dr. TETHER. One question I am asked is whether DARPA's efforts are aligned with DOD's priorities.

DARPA's well aligned with DOD's efforts to transform itself. Ninety percent of our budget is—over the five-year defense plan maps into the six Quadrennial Defense Review (QDR) operational goals for transformation directly.

In fact, of the ten percent that does not map, five percent of that is Basic Research and 2.5 percent is Small Business Innovative Research, which we could have actually put on there, but we did not. So this is a very specific mapping.

Another question that I am asked is what is DARPA's methods for transitioning technology and is it successful.

Let me mention how we get our technology to the warfighter. There are basically three basic ways.

One, DARPA is a very low-overhead operation. Over 97 percent of our money gets into the hands of the performers—industry, universities, so forth and so on.

And what we do is we develop capability in industry. We develop capability in industry until industry is brave enough to bid that technology to somebody other than DARPA.

Now that occurs—in order for that to occur, industry both has to have the capability, but they also have to believe there is a customer who is going to receive it other than DARPA.

So our second method is basically all of our money—almost all of our money is contracted through the other—the Army, Navy, Air Force service and technology organizations.

This is where the COTRs are, the Contracting Technical Representatives, who basically are—by doing this, we are building up a constituency in the services, and, as time goes on, the industry has the capability the constituency has built in the service, and the transition occurs.

And usually, at that moment, DARPA is totally forgotten about, as well it should be, actually, in order to have that transition be successful.

A third way when we actually go and try to build a prototype system—go all the way, not just build the capability, but actually

build a prototype system—is we develop memorandums of agreements with the services.

And what we try to do with the memorandums of agreement is to come to an agreement which says something like, if I build this capability in 2007, you promise to put into your budget money in 2007 and the out-years to take it over at that point.

Basically, we have learned that if you cannot put money in 2007 in 2004, you are never going to put it in 2007 in 2007, and so this is one way to avoid that gap that sometimes occurs when we build a prototype system.

Now, to help all of this work, we have liaison officers from each of the services, from the Army, Navy, Air Force, and Marines, that live at DARPA, and their job is to go around to DARPA—the program managers, understand what the program managers are doing, and to basically be—spread that word to the services, also bring back from the services—the respective services the needs, you know, what is it that they really need, not requirements but what they really need. You know, what is it that is not written down that really is needed.

In addition to that, we have memorandums of agreement with Joint Forces Command (JFCOM) where JFCOM is going to actually put a liaison officer up at DARPA, and we are going to—on a—this is a new thing—on a—in order for DARPA and JFCOM to be able to transition technology that way.

We also have a liaison down at Special Operations Command (SOCOM). Here, we did not ask SOCOM. We just went and did it. We just went and put—and this is very unusual for DARPA to do. This has been done in the past.

But this is very unusual to—for—we just put a person down there, a DARPA person at SOCOM, and the job of that person is to really make sure that DARPA technology and the SOCOM needs are well known.

And, in doing so, over the last six months that we have been doing this, we really have a great list of technology that is being transitioned into SOCOM.

Now we like SOCOM. We like SOCOM because it gives my program managers almost instant gratification. The toys that develop—the capabilities that we develop, SOCOM will go out and experiment with and give us some feedback, and if we develop 10, 20, 30 of these things or—it is almost all they need, so we get an instant feedback from that organization.

Now, when we met a few weeks ago, I showed you a history chart detailing some of the major DARPA transitions over the last 44 years. That chart, however, did not directly include the massive information technology efforts transitioned by us because it is very difficult to get a picture of that.

A review by the Department of Defense IG, Inspector General, of the transition of our information technologies found that we did a good job. I gave a copy of the IG report to the committee staff. Jean has a copy of it.

Basically, the IG stated that DARPA is successfully pursuing new information technology programs and the technology is being transitioned to military and commercial users because the program

managers were effectively planning, managing, and coordinating with potential users.

IG, however, in their way, they could not just say something nice like that and leave it alone. They had to close with saying, well, we needed to continue to focus on the warfighter. So, when you read the report, there is that part in there, too.

Soldiers in the field—today, Mike showed you a—this organic aerial vehicle (OAV). I had shown you a model of it. This is the actual OAV. This is—they would not let me have one that had a motor in it, but this is the actual OAV. That one flies.

And, if you look at, there is a camera on the front, and there is—if you look at the bottom of it, you will see a camera and two other ports which have a wire over it.

The reason—the camera on the bottom—the purpose of the camera on the bottom is to be able to—so the soldier can see where the edge of a building is and then basically put a land command that lands—the other two sensors are acoustic sensors which basically tell that how far off the edge of the building is so it automatically lands and then perches.

And with that, we can populate a city—an urban city and basically see what is going on, which—and is really one of the greater difficulties.

We also have a water pen. This is in use today. This is in use in Afghanistan and also in Iraq.

Basically, its obvious use to people who need water—water is one of the biggest logistics burdens that we have, but, by having that pen basically allows soldiers to use water wherever they find it and be assured of its—that it is safe.

And, again, the Marines are now setting up a program to purchase that pen in large quantities.

Finally, we have a Phrasilator—Ron has it over here—which allows a warfighter to speak into the hand-held device and have the phrase converted to any of several languages.

Last night, ABC “World News” had an interview with a Marine in Iraq using that Phrasilator when he had captured some prisoners, and he used the Phrasilator to communicate with the prisoners to ask them if they had any—whether the prisoner was wounded.

Obviously, that Marine did not know anything about the DOD’s Science and Technology Program, probably never heard of DARPA and Director of Defense Research and Engineering (DDR&E), whoever, but it does not matter. I mean it is in use and—today.

Finally, I am often asked what is the most difficult part of my job.

Finding new people to come to DARPA is one difficult part. We rotate program managers at the—by design at the rate of 25 percent a year. That is our turn rate. The program managers at DARPA are really there only four years.

However, Congress, you all have really helped me to be able to bring new, good people into DARPA by providing what is—we call the Section 1101 hiring authority, which was established in the 1998 authorization bill, where we can literally hire as if we are an industry.



I can make an offer to somebody and have them working that afternoon. Now that is exceptional in the Federal Government, and that is really what was referred to earlier as a capability that the labs now have.

We have 40 slots, and we basically have filled up 38 of them.

But the important thing is that when you have real good people—as I told you once before, we do not have jobs. We hire people for their ideas, and when, you are hiring people for their ideas, to be able to say, well, listen, I would like for you to come, but it will take me six months for me to get you in here is inconsistent with DARPA.

So this really is a capability that you all gave us, which is—without it, I do not think I could do this job.

Second of all, the last—another difficulty is making sure that I—it always bothers me—I am trying to always make sure that we are reaching out for those people on the far side and not just going to the same old people, not that the same old people are bad. I mean, they are good people, but I really worry about am I really getting to the new people who do not know anything about DARPA, never heard anything about DARPA.

The prize authority that you all granted last year or renewed actually last year, is helping tremendously. We are using it to hold a contest in the desert next year of autonomous ground vehicles, which, obviously, play—extraordinarily important to the Army. They—the challenge is to go from outside L.A. to Las Vegas, and the one who gets there first is going to win \$1 million, winner take all.

This is an exciting way to get new people. I mean we have had people become interested in this who ordinarily would not even think of being involved with the Department of Defense.

Other ways we do this—we hold a conference every 18 months or so. We held one last year in Anaheim, Disneyland. Where else could you hold a DARPA conference but Disneyland? Or Disney World would probably be okay. And we are going to do this again in another year. We had nearly 2,000 attendees at that conference.

And then, finally, I spend an awful lot of time giving briefings at conferences and universities all around the country to make sure that people know about us.

But there are many other questions that I am asked, but I think, at this point, I will just thank you very much for your support in the past and your future support, and I will close and look forward to answering your questions.

[The prepared statement of Dr. Tether can be found in the Appendix on page 232.]

Mr. SAXTON. Well, Tony, thank you very much. We—we appreciate what you do, and we know you have got a tough job, and we are very grateful for the—for the great effort you make.

We are going to let Jim Turner ask the first round of questions here.

Mr. TURNER. Thank you, Mr. Chairman.

And I certainly am encouraged by what I hear from each of you. It makes us proud of our military. It makes us very much aware of why we do have a decisive advantage in battle.



Dr. Tether, we have talked at a previous meeting about a subject that I would like to address once again because it is certainly an issue that is on the minds of all of us right now, as we engage in the conflict of Iraq and know that there is a heightened threat of terrorism here at home.

One of the most serious threats, in my view, that we face, the one that—in addition to possible nuclear device detonation, the most serious threat that could result in the greatest loss of life is the threat from bioterrorism.

And I know that you have told us before that you have done significant work at DARPA in that regard, and I would like to approach this by asking you to address a question from me, and you can share in your answer what you are doing, but I—perhaps my question to you is even a broader challenge than what we are currently doing.

But I would ask you if we were to make a list that could be agreed upon as being the 10 most serious biological threats that could be used both against our own troops in battle as well as used against the people of our country here at home, I assume we would start with things like smallpox and anthrax and botulism toxin and on down.

But if our goal was to develop the vaccines and to develop the antibodies, to develop the drug treatments that might be necessary to deal with those threats—if that was our national goal, how would you suggest we best organize ourselves to find the answers to those threats and to find them in a way that we could not only do the necessary research to find the proper vaccines, proper treatments, but we also could have assurance that once we find them that they could be rapidly manufactured and deployed and put in place and stockpiled so that they would be available either to be utilized in advance or to be utilized at the time an attack occurred. But what would your view be on how that would best be accomplished?

And I know, in your work, you have worked with universities. You have worked with the private sector. You are very familiar with the capability of our government agencies, in particular the department. But give us your view on how that best could be accomplished in the most rapid fashion possible?

Dr. TETHER. Well, thank you again for the question.

The problem that I see in being able to do what you said is really not in the early stages of finding the drugs. We have a good program going on with the Department of Defense where we are working hard on finding vaccines for all of the diseases that you have talked about or therapeutics, if somebody has the disease.

And the techniques that we have been using are—we have deliberately made them quite different than the way the big pharma does it today, and what we have done, as I mentioned in the last hearing, is our approach has been to try to find one drug for many bugs by really looking at the bug itself to get down to what makes this bug different.

And it turns out that the bugs you are talking about, if you look at their DNA, all have a content of AT, which is part of the DNA, which is well over 80 percent where humans are like 10 or 15 percent.

So, by going at that and attacking them that way, we believe that we can come up with drugs—and we have—that basically will go after those bugs but also will not allow those bugs to be genetically changed because we are going after a part of the bug that you would not be able to change.

This—I mean one way to think about it is if I find a way to rip out your stomach, you are going to die, you know, and you can genetically change your brain all you want, but as long—if I go for your ability to put energy into your body, you will not survive.

The reason we did that that way is that what we are hoping to find is a commercial bug—the common cold would be perfect—where if we could find that to be one of the bugs, then we could get the pharmaceutical companies to basically take on the real hard task of how do you get these drugs, as you said, so that they are allowed to be used on humans.

The manufacturing costs to put them into manufacturing is very large, and that is where—I do not—honestly, I do not have an answer, but that is where I see the difficulty is. I do not see the difficulty—I do not think I would change a thing on the front end, on finding the innovation of the new drugs.

But what we have problems with, what the department has problems with, is how do we go to the next phase in the FDA, you know, phase two, phase three trials, and then getting somebody to spend a lot of money. And it is a lot of money to create a drug line.

If we—if this—you really wanted to take this problem seriously, then I think what has to be done is that the Federal Government would have to put down the money to basically have somebody decide—and I do not know who that somebody is—homeland security—but somebody needs to decide here is something that really has the potential, and now we are going to just pay the money to get it through the rest of the trials.

None of us have that kind of money. The S&T people I am talking about. None of us have that kind of money in our budgets to take those inventions any further.

I do not know how to organize that. I do not know who should do that, but that is what really needs to be done to do what you want to do.

Mr. TURNER. Could the private sector, could the private drug companies be incentivized in some way to take on that responsibility?

Dr. TETHER. Well, I think so, and I think that is what has to happen. Now one way to incentivize them is just to pay for it. You know, I mean literally just pay for the cost of doing so.

You all know far better than I do, you know, how—I mean tax breaks is another way to incenti—but—yes, I think they can be incentivized, but they have to be incentivized and I do not mean, literally at the monetary level.

Mr. TURNER. So you are saying that, within government, within DARPA, within in the—I guess the other capabilities, National Institute of Health, we have the capability to determine the kind of vaccines, to make those—to do that research and come up with the right answers in terms of what the treatments are and what the vaccines should be.

Dr. TETHER. I believe we do, but we do not have—we do not have the money or the wherewithal for the next step. You still lose a lot of these drugs when you go to—you kill—it kills the bug, but does it kill humans?

You know, I mean it is sort of like the operation was a success, but the patient died, and that is sort of what these trials are about. I mean they are there for a very good reason. I mean there was a lot of things that we have developed that literally kill the pathogen but also do bad things—side effects to humans.

So the trials are really trying to find the answers to all—and they are very expensive because they do end up having to become human trials.

Mr. TURNER. If you reach that stage you just described and you tried to entice a private company into taking it from there and moving it forward, and to try to entice them to do so, you offered them in advance a guarantee that you will contract with them to buy several million vaccines or doses or whatever so that they knew at the end of the day they are going to be able to sell whatever they end up producing—

Dr. TETHER. That is one way of doing it, although then they still have the risk of what if it did not work. You know, you can be \$300 million, \$400 million into these trials and then find out that it was—you know, it was something that did not work.

I really think that we need to almost—as we do with ships, airplanes, missiles—you know, when it comes down to something which is really something that we need for our national security, we have yet to ask, although every now and then we do try, a company to go build an airplane on their own hook, and then we will buy it from them. You know, we literally end up having to pay the freight for having that airplane developed all the way, and I think we need to look at this problem the same way.

Mr. TURNER. So you think it would be better if we as a government went ahead and committed the funds to try to move this forward to the point where there—we were capable of moving into production and then pay for the production, and then it is available—

Dr. TETHER. Absolutely.

Mr. TURNER [continuing]. Stockpiled for use.

Dr. TETHER. Absolutely. And that is exactly what we do with every other weapon or defense system in the Department of Defense.

Mr. TURNER. If you took the other approach I suggested and simply provided a private company with a contract in advance guaranteeing them a certain amount of money if they were to bring this vaccine through the clinical trial stage and on into production, let's say for botulism toxin, then would it be a reasonable concern that we might have placed all our eggs in one basket if we just made that one contract with that one company that—

Dr. TETHER. No, I think the contract that you are talking about—they first have to come up with it, and then we will buy it. But a company then has to assess the odds of them coming up with something, and then—you know, so that you will buy it, and that could be done.

But then that, again, is like us going out and saying, look, I have a—I want you to—Northrop tried this one time. I want you to build the F-22, I think, is what the airplane was.

I do not know, Jean. Do you remember?

And if you build it, we will buy it. Well, they went and built it, and we did not buy it. I mean they put down a lot of money, and it—the DOD chose to not buy it after they had it.

So you have got to—if you really want to solve the problem, I think you just have to go and do it the way we do it. There is a good reason for why—you know, for things that are not—for things for which there is no large commercial market, and we really are the customer. We—I think we have to pay the freight.

Mr. TURNER. We have to pay the freight—

Dr. TETHER. All the way.

Mr. TURNER [continuing]. Paying for the cost of development right on through paying for the cost of production.

Dr. TETHER. All the way. All the way.

Mr. TURNER. And if you guarantee a private drug company that, at the end of the day, if they took it through the clinical trial stage and on into production, if you guaranteed them in advance that you were going to buy what they produced, I guess you could be buying a pig in a poke.

Dr. TETHER. Well, no. I mean, obviously, you would only buy it if it worked. But what you are asking them to do is to put the bet down, to spend \$600 million to see if this particular technique really worked.

Mr. TURNER. So you are saying then it would be really foolish to contract in advance to buy something when you do not for sure whether what is going to be produced is going to work.

Dr. TETHER. If you were a company, a pharmaceutical company, you would be foolish to take that contract, unless you knew—

Mr. SAXTON. If you will yield to me for just a moment

Mr. TURNER. All right.

Mr. SAXTON. You mentioned \$600 million. Is that a number you used or is that—

Dr. TETHER. It is a number I have been told of what it takes to get a drug from, you know, like discovery all way to—through the FDA process to manufacturing in large quantities. I have not verified—I am just giving you a number I have—

Mr. SAXTON. For less than a billion dollars, you think we can solve the biological—

Dr. TETHER. Well, let's put it at a billion dollars per attempt. I mean it is less than a billion dollars per drug, and that is where the rub is, you know.

Mr. SAXTON. Well, you would not mass produce drugs—a drug if it did not work.

Dr. TETHER. Well, we—you do not know it does not work until you spend a lot of money, is the problem.

Mr. SAXTON. I understand all that. But when you answered my question on the \$600 million, I thought you said that it included production of the drug.

Dr. TETHER. Right, right. So that is—you are right. If you—if we got to the point where it did not work, you would save some of that \$600 million, and probably it is a third of it anyways or a half.



Mr. SAXTON. Okay. I——

Dr. TETHER. Do not take my numbers—you know, I——

Mr. SAXTON. No, I understand. We are just—we are ballparking here.

Dr. TETHER. Yes.

Mr. SAXTON. Yes.

Mr. TURNER. I know I have taken too much time. I want to—just one other question to clarify something in my mind. It is my understanding that, in the State of Arkansas, we have a Department of Defense facility that actually manufactures—is a manufacturing facility. It may be a facility that is where we contract with the private sector to produce, but tell me what kind of facility that is and what its capabilities are if you are familiar with it.

Dr. TETHER. I am really not. Where is BioPort? BioPort is the—Excuse me. Chicago. BioPort—BioPort is a company that is making anthrax vaccines for us, and, basically, you know, they are making it, and we are buying it, and we have a—we buy it by the shot, I guess.

Is that the way it goes?

But I do not know—I do not know about the company in Arkansas.

Mr. TURNER. Thank you very much. You have been very informative.

Mr. WILSON. Thank you, Mr. Chairman.

And, Dr. Andrews, I was very interested to hear of the effort to reduce the soldier's physical load from 90 pounds to 40 pounds, and I just think that is excellent, and—can you get any more specific on how that would be done?

And in particular, last week, the chairman arranged for an extraordinary presentation about the new protective gear and gas mask, which now we have seen so often on television, and the progress there was so encouraging, and what you said is—it sounds astounding.

Dr. ANDREWS. You have to attack the problem. Right now, it is 92 pounds of carrying a fighting load in, which carries your ballistic protect, your water, your other part—your ammunition, your overall equipment, your computer, your communications system, and part of the challenge we face here is how to redistribute some of that fighting capability across the squad, let's say. As a system of systems, you do not count on just one piece then. You distribute—people carry different items along the way.

Part of it is the power and energy, as Dr. Segal talked about a moment ago. Very—very importantly, right now, we carry—I do not have the numbers in front of me. A very significant piece of our weight is the batteries to power all of our electrical devices, and part of the thrust to get at this now is using hyperelectric in terms of fuel cells.

Essentially, how do we propose to—if we can burn methane on the battlefield inside one of these fuel cells, you save the power—you essentially save the weight associated with the power density of the battery.

We are also pursuing efforts in what we call microturbine engines. If you burn diesel, you essentially replace the—a battery—



a standard battery with something that is the size of a dime. That is a bit further downstream.

So it is essentially replacing the armor with lighter-weight materials, distributing the communications systems across the field, counting—using the networked fires like you saw displayed up here so that soldiers can call in fire from the precision attack missiles so they do not carry as much fire power with them, if necessary. They are going to get sent with only the right kinds of solutions in place and a lighter-weight rifle, let's say, for the future piece.

Mr. WILSON. And in particular, in communications, I am still hopeful that each troop could have the equivalent of a cellphone rather than other systems that I have seen. Is that where we are going?

Dr. ANDREWS. Yes. In fact, if the last shot is a technology that came from DARPA, and it is called a small unit operation situational awareness system, and it was a—it was that big thing carried on the soldier's back at the moment because that was a prototype.

Mr. WILSON. Right.

Dr. ANDREWS. We now have a three-year effort, which is part of the soldier program. It is to reduce that down to a—essentially a very small size, hand-held size, and that is the—ultimately going to be what is called the Tactical—the Joint Tactical Radio System, and it is the—essentially the surrogate for it until that comes on line, what they call cluster exident. So what you saw in terms of ability to communicate on the battlefield, both across the squads and up the echelon level, is that kind of capability.

Mr. WILSON. I think that would be very helpful.

And for Dr. Segal and Dr. Tether, there has been so much coverage today about the capability of Iraq with their radio and television transmission, and I had thought that there was a capability of some type of electronic pulse or some type of jamming device that could have effectively knocked out a country's propaganda machine without having to resort to an actual attack. Do—does such exist?

Dr. SEGAL. There are a variety of options that one has of going against communications systems, and I think this is probably not the right forum to go into the other options.

Mr. WILSON. Well, I—because I did not—it did not surprise me that Iraq has—or Saddam Hussein has a child-care center next to the television station.

Another question for either one who may apply or be able to respond. All of us are concerned about friendly fire, fratricide, accidents, and the accident that occurred this week with the Royal aircraft and the Patriot—has there been any determination, even at this early stage, as to how that occurred or how that could be avoided?

Dr. SEGAL. I am personally not aware of the results of an investigation into that friendly fire accident.

Mr. REED OF THE COMMITTEE STAFF. If we can get that for the record—

Mr. WILSON. That would be fine, but I just—something that is elementary as a returning jet to be fired at by our own Patriots, it was certainly tough for all of us this past weekend.

I have no further questions.

[The information referred to can be found in the Appendix beginning on page 293.]

Mr. SAXTON. Mr. Kline.

Mr. KLINE. Thank you, Mr. Chairman.

Thank you, gentlemen, for coming today. I know it is late in the afternoon, and the questions grow long. A couple of quick ones.

Dr. Segal, a few—couple of weeks ago, Dr. Tether was testifying, and we were talking about the level of effort spent in chem-bio, and put into the context—the larger context, if you will, of your—your fifth piece here called accelerating the support to the war on terrorism, looking from your position across DOD, where would you say we are at level of effort of the—of S&T on that war on terrorism, particularly chem-bio but a broader range, if you choose. Where are we?

Dr. SEGAL. The war on terrorism has many, many parts, and some of the systems that I mentioned—in fact, if we would be able to load that—I have a CD with one image of a short—very short clip of this Thermobaric Hellfire missile as an example of how we are approaching certain targets in a very surgical way, and, if we bring that up, it is designed to be very effective in enclosed spaces, whether it be a multi-room structure or a cave or other enclosure.

If we can bring that up—this is from a Cobra. It is a multi-room structure, and the goal was to attack one floor of the building but not harm the upper floor, and so, in that case, whether applicable to kind of an urban-type environment or others—so there are systems that were—would be surgical in terms of urban warfare.

There are systems for looking in terms of developing technologies, which we have accelerated, in agent defeat, whether it be in terms of chemical or biological stores, and we have developed capability in those areas working toward a systems for detection of chemical, biological, and radiological kinds of agents, and we have accelerated the development of those as well for the global war on terrorism.

Improvement of communications systems is also very important. Tony Tether mentioned the Phrasilator developed by DARPA, but now incorporating it in an Advanced Concept Technology Demonstrator (ACTD). Some of the technologies incorporated a program called LASER, and the technologies to Language and Speech Exploitation Resources is the title of the ACTD. Software package of reading and hearing foreign text and translating into English.

It—I saw the demonstration of that actually today and an Al Jazeera article that was translated automatically into English, and the Phrasilator allows, as was demonstrated, English, then into a variety of languages to be brought to bear on the global war on terrorism.

So your question was in terms of level of effort, but it spans information technology, it spans weapons systems, command and control, communications, computers, intelligence and so forth, in addition to the chem-bio-nuclear pieces.

Mr. KLINE. Excuse me. I take your point. I guess my point is that, in different decades, at different times—you could say that there was a large level of effort, for example, on Stealth, or, at another time, there was a large level of effort on communications and

simulators. It seems to me that we are in this war on terrorism, and, as the president said, it is going to be a long war.

So, granting that there are multiple applications in conventional warfare and the war on terrorism, I am just wondering if you feel that the level of effort across the span, the services, DARPA, DTRA, all the things that you are looking at—are we putting the right level of effort into the war on terrorism? Is it enough? More—do we need more money? Do we need more focus? What is your sense?

Dr. SEGA. I believe we are putting the effort on the global war on terrorism. We have—in the near-term, monies and flexibilities that we have is—almost exclusively from my office has been pointed to the near-term needs of Central Command (CENTCOM), Special Operations Command (SOCOM), Northern Command (NORTHCOM).

Now the broader question in the global war on terrorism also includes the defensive piece in homeland security, and other partnering agencies are very important. So in the—in the bio piece, DARPA has a significant program in biology. But so does the National Institute of Health, Health and Human Services, and so forth.

And so the partnering arrangements are very important, and we are engaging agencies and organizations outside the Department of Defense to make sure that we have integrated our research and development with that in other parts of the department—of the Federal Government.

Dr. TETHER. Okay. If I could take a moment. I—I am sorry Congressman Turner left right—I do not think I really—I can use this as an example of—last week, I told you we spent about—that—if you add both the biology, and the detectors about \$300 million, or 10 percent of our budget, and I think I said that, if this was a space program, it would be equivalent to something three times bigger.

Well, I went back, and I thought about that a little bit more, and I think I was off. It really would be equivalent to about a billion-and-a-half-dollar space program, and the reason is—and this is what I did not make clear—the reason is that, in the space program, this \$300 million is sort of equivalent to the front-end design and research, and then we take it the rest of the way.

In other words, in the space program, I would then take that technology and actually build a spacecraft and launch it and test it and do all of those things, and that is why it is a billion and a half, but, in the biology, counterterrorism, we stop. We stop and we do not have any way to go and get the \$600 million to bring it through the FDA process.

In other words, the—in the S&T part, we are doing our thing, but there is not an equivalent acquisition system that takes what we have and brings it the rest of the way. I mean we are hoping on the big pharmas to do it for us, but we do not do that on the rest of the stuff that we build. I do not know if that helps, but—

Mr. KLINE. Oh, I—it does help, and it seems to me that Mr. Turner was working—needling, if you will, on a problem that we need to address. We need to—we need to protect the homeland, we need to protect American citizens, and we cannot let a process, if

you will, or lack of a process maybe, prevent that from happening, and I appreciate your stepping in then to expand on the answer from the question before, and it does bear directly on what I am getting at.

And the reason that I asked Dr. Sega is I was asking for the look across DOD, not that DARPA does not look across, but, in your role, are we—are we addressing that? Are we going to get to where we need to go? And chem-bio is at the top of my concerns, but there are other—other things in this—in the war on terrorism—we just looked at a pretty neat little Hovercraft here, for example—that the emphasis is there and not on a radar cross section or something like that.

Dr. SEGA. Well, the—to bring a, I think, cohesive look at the ability of the research and engineering community to bring to bear our—what we have available to the war on terrorism was the motivation for forming the Combating Terrorism Technology Task Force in the first place.

And so it—it is at the leadership level in the services and agencies, as well as our partners outside the Federal Government, to look at that and also bring in the folks that are actually fighting the war on the battlefield—and it is a varied battlefield, obviously, in the global war on terrorism—to see if we are getting this right.

Mr. KLINE. Okay. Thank you very much.

I have a burning question for Admiral Cohen, but I see my time has long since expired, but I would like to talk to you about my mine countermeasures at another time.

Thank you, Mr. Chairman.

Mr. SAXTON. Before we go to Mr. Langevin, I just would like to follow-up on John's question because I am not—I am not sure that we collectively are devoting the resources that are necessary to the war on terrorism.

We are good at doing what we do. We are good at fighting conventional wars. We have been fighting conventional wars since the beginning of time, and we are—for example, over the next several weeks, we are going to show our capability of fighting a conventional war, and I would make the point that there is nobody in the world today that can fight a conventional war like we can fight a conventional war.

And yet the major program that we have discussed so far today is the Future Combat System, which is a conventional—scientific, highly technical, conventional combat system, and we have got this war on terrorism to fight for.

Let me ask you this question. How much money are we—how much of your budgets are we spending on information collection? We have been briefed by so many people who are fighting the war on terrorism that we no longer need the conventional capability that we needed during the Cold War. We all know that. We have got a different enemy. We need a small force to meet this enemy, but we need a huge collection system to know where he is so we can go get him.

How much of our budget are we using on information—are we using trying to develop new ways to collect information on our enemies?



Dr. TETHER. Well, you know, we are—we have a program called Terrorism Information Awareness (TIA), which we have talked—

Mr. SAXTON. We know that. [Laughter.]

Dr. TETHER. But it is—it is addressing, you know, that problem. It is—

Mr. SAXTON. Okay. How much—

Dr. TETHER. It is not—

Mr. SAXTON. How much of your budget is TIA?

Dr. TETHER. It is another five percent.

Mr. SAXTON. Five percent. Okay.

Dr. TETHER. But, again, it is—it is a non—

Mr. SAXTON [continuing]. Information—is that—okay.

Dr. TETHER. It is a non-hardware program.

Mr. SAXTON. It is really information coordination, and I will accept that as part of information collection.

Dr. TETHER. Yes.

Mr. SAXTON. Anybody else have any information on intelligence gathering?

Dr. SEGA. The third cost-cutting initiative that I had mentioned was in the area of surveillance and knowledge, and that is the one that we are in the process of pulling together, but the—I would like to take the specific number for the record to try to—

Mr. SAXTON. Yes, I am—

Dr. SEGA [continuing]. Get our arms around that, but—

Mr. SAXTON. I am just trying to make the point. Look, I have been doing this since 1987.

Dr. SEGA. Sure.

Mr. SAXTON. It took me 17-1/2 years to get Congress' attention, and we still would not have—so I am not picking on you. I—

Dr. SEGA. Sure.

Mr. SAXTON. I am picking on Congress, too, because it took us 17-1/2 years after I started doing it, and there were undoubtedly people before me trying to tell Congress that we needed to address the subject of terrorism. We are good at doing what we like to do. We like—That is the wrong way to put it. We are good at doing what we are successful in doing, and we like to be successful in fighting conventional wars. This is no longer a conventional war, and yet—and I am not saying this to you as individuals—I do not think we are addressing the issues that we need to address to fight the war on terrorism.

How much money are we spending—how much of your budgets are we spending on developing—solving the problem of biological warfare? It is blank. And they are—whatever other aspects of terrorism we need to address. And maybe the question is how can we help you with those issues. Do we need to restructure? Do we need to have an agency that does research on these issues that are peculiar to this—to these subjects?

Admiral.

Admiral COHEN. Mr. Chairman, I appreciate—

Mr. SAXTON. I am not really this mean, you know.

Admiral COHEN. I appreciate that Dr. Sega's asked to take the question for the record, but we are doing an awful lot. I am sorry that Congressman Turner is not here.



You know, our surgeon general and our Navy doctors have been working diligently on what we used to call DNA and we now call vaccines. It is a variation of what Dr. Tether talked about. I will tell you that those Navy captains, those Navy doctors—and we will get this right.

We are close to going into human trials—is you take the DNA of whatever the antigen is. We then tailor in weeks the vaccine. We can test it, get it out there, and then, when the bad people modify genetically that, we modify the agile vaccine to go back toward that. It is scalable. It is expandable.

Those doctors, I believe, will be competing within 10 years for Nobel Prizes in medicine. There are lanes. There are lanes. And I spent a lot of time with these other gentlemen.

And we have a lot of cost-cutting areas, but it is the Congress that has established in the Department of Defense chem and bio now under Dr. Anna Johnson-Winegar with a significantly enhanced budget that you all provided. We also have National Science Foundation (NSF). We have the National Institutes of Health.

It would be my hope that, as the Homeland Security Department becomes organized, and I believe that will happen, having worked for Secretary England when he was secretary of the Navy, that he will leverage all of these various investments, which are very significant and are focused to address the very things that you need. We have a strategic level.

We have a tactical level. We have an offensive and a defensive mentality. It is a difficult question. You are—I salute you for bringing it up. I do not think we are going to resolve it right here.

Mr. SAXTON. Yes, I agree with you. Jim. Oh, I am sorry.

Dr. Sega.

Dr. SEGA. Perhaps another part of your question is that in terms of the intelligence. Just recently, we have a new undersecretary of defense for intelligence, Dr. Cambone, and we have met with his developing organization to make sure that we are going to align technology investments in that very important area in the department as well.

Mr. SAXTON. Thank you.

Jim. Jim Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Gentlemen, I want to congratulate you on your testimony today. It is been very informative here.

First, I want to just go to Admiral Cohen and just comment on your mentoring program, and I am very pleased to hear that you are doing that. I mean, for a while, I have been concerned that we are not investing enough in science and technology, most importantly in terms of bringing people into those fields.

And that was certainly confirmed by the findings of the Hart-Rudman Commission, which, as you know, was an historic commitment between President Clinton and Speaker Gingrich to evaluate U.S. national security in the 21st Century, and that report concluded that we are putting our own national security in danger by not investing officially in those deals and bringing people into the fields of science and technology.

So it sounds like a great program. I encourage you to continue that.

If I could—I have addressed you, Admiral. I know that, because of this global war on terror as well as the Iraqi conflict right now, much of the American public has been introduced to the capability of unmanned aerial vehicles, and it certainly has enabled our troops to carry out their mission more effectively, as well as making great strides to protect our troops.

And I understand that we are also—DOD is also developing unmanned underwater vehicles, and particularly since I have Newark in my home state of Rhode Island, I would just like to ask if you would give us some progress on these programs and talk about some of the advantages that those programs have over manned vehicles.

Admiral COHEN. I—yes, sir. And thank you so much for your comments on our initiatives with S&T. We are not as fancy in the Navy and the Marine Corps as some of our brethren services. We still use pasteboards. But unmanned vehicles in all of our services, in all agencies, are absolute critical, and you have seen some examples of that today.

Tim, if you would get out of the half torp, I think I would prefer that.

We have gone ahead and provided the Remote Environmental Monitoring Unit System (REMUS), which is a small unmanned underwater vehicle currently in use in the Persian Gulf. As you know, although we have captured the port several days ago, there is a significant mine-clearing effort that is going on before the full amount of relief supplies can get in.

What I am showing you here, Congressman, is what we call half torp. As you know, Newark—at Newport, it was key in developing the old torpedo station, the Mark 48 torpedo. When I took over three years ago, it was clear to me that mines would be a very significant threat to our submarine operations.

Out of 688 submarine carriers, 26 Mark 48 torpedoes. We had not significantly improved the head, meaning the hydrofoam on the torpedo, in some period of time. We have had incremental improvements, as you can imagine.

What we did was we came up—worked them into it with the half torp. The half torp is half the length of a Mark 48 torpedo, using the conventional propulsion, less one inch. So, instead of 26 rounds in the 688, we could carry 52 rounds.

As you can see on the left-hand side or your right-hand side, we changed the head to be scores of small hydrofoams instead of the classic four-quad hydrofoams, and you can see the difference in definition from the top yellow to the bottom pink showing in a countermeasure environment how it can discriminate a target.

We designed this to find a one-meter tethered mine in the littoral, which has great reverberation, in a countermeasure environment, and what you see on the bottom on the left is what the Mark 48 torpedo sees today. You cannot discrimination a target.

On the right with the new warhead, you can see not only the countermeasures, which are those red vertical lines, but the target farther to the right. Newark turned this around in 18 months. This month, we are shooting the first of these at Ortech, having vali-

dated at Lake Seneca. Those are side-by-side in-water validations. So this is just one example of how unmanned underwater vehicles—this was a weapon that we have refined.

The REMUS is a sensor to find the mines. This can find the mine and destroy it at the same time.

Mr. LANGEVIN. Thank you. I guess my time has run out, so I will—thank you again.

Mr. SAXTON. Jim, you—you have been patient. Do you want to take another minute? It is okay.

Mr. LANGEVIN. Well, if I could since, Chairman, you raised the total information awareness (TIA) program, you made mention of that, I was wondering if you could briefly talk about it—I suppose we know what it aims to accomplish, but do you want to talk about that as well as its current operational status and possible practical applications.

Dr. TETHER. Well, TIA right—it is in a very—it is a research stage, and it does not—regardless of what you may have read in the papers, it really is not a collection program. We are not collecting any data. We are not spying on U.S. citizens.

Basically, what TIA is doing is providing tools to allow agencies to better collaborate with each other. I have been involved in the business for a long time, and, every time I have seen an intelligence failure, it was never because we did not have the data.

We always ended up being able in the forensics to show that we had the data. It is just that the data was distributed. CIA had some. NSA had some. DIA had some.

But the problem was that there was no technology which allowed them to collaborate with each other so that they could bring their data forward to solve a problem, and that is all that TIA—the research in TIA is about, is really to do that, to allow agencies to communicate with each other and collaborate, and yet maintain the privacy of their sources and methods.

It is an experimental phase. We have—we have—we are doing a spiral development.

United States Army Intelligence and Security Command (INSCOM) is a major node. Now INSCOM is not just a single place. INSCOM is worldwide, and, basically, we are learning how to use these tools, and it will be many years before it—you know, it really is to the point where it needs to be.

I do not know if that answers your question or not, but—

Mr. LANGEVIN. That is helpful. Thank you.

Thank you, Chairman.

Mr. SAXTON. Is—on that—on that same question, is—is the research project active and aggressive in regard to TIA?

Dr. TETHER. Yes, it is. Very active and aggressive. In all fronts, in language translation, in being able to create models.

Another misunderstanding of TIA is that it is thought—some people thought it was a data mining thing, that we went out and went into databases to look for patterns. Actually, it is the reverse.

The—there are two technologies—major technologies. One is the collaboration technology, but the other is to make things from a hypothesis-based or a model-based—where you create a hypothesis and you say, if this hypothesis is true, what are all of the observables that have to be true.

And then you take that pattern to the database to see if they exist.

Mr. SAXTON. Have we gotten past the public relations problem?

Dr. TETHER. I am getting less letters. [Laughter.]

Mr. SAXTON. That is a good thing.

Admiral COHEN. But they are catalogued. [Laughter.]

Mr. SAXTON. Todd Akin.

Mr. AKIN. Thank you, Mr. Chairman.

I had a couple different things, but some of the other questions, so I figure maybe—the first one on the Mark torpedo—do you use one Mark torpedo per mine? That is kind of an expensive way to work at things, isn't it?

Admiral COHEN. You know, it is a lot cheaper than using one submarine per mine.

Mr. AKIN. Yes, that is—yes, the—relatively speaking, I suppose. [Laughter.]

Mr. AKIN. And that is what you are talking about with that technology.

Admiral COHEN. That is correct. But the real effort here was, if we can find a one-meter mine tethered in a littoral, which is a very difficult sonar environment, we can find a seven-meter-diameter submarine. If I scaled this to find a seven-meter submarine, it was no guarantee I could find the one-meter mine.

So I set the goals high for the smaller object with the real intent not being the minefield because we have many ways to find and destroy single mines, especially in the littoral. This was to be able to have the load to defeat the submarines that we might encounter.

Mr. AKIN. Okay. That explains—that makes the American taxpayer—at least this one feel a little better anyway.

I was going to ask—I think, Dr. Sega, it might be in your area, but some other—some of the other gentlemen as well, and that is the hypersonics area. We have been interested in that, and I am from the St. Louis area where we have got Boeing working on some of that.

Could you give us a quick update because I understand that from a—you know, a shuttle vehicle as well as defense against cruise missiles that are moving at more than speed of sound and then, of course, just from a flight point of view, where are we on that in the hypersonics area?

Dr. SEGA. Last year was a big year for ground testing propulsion systems in the hypersonics area, and I will probably let others expand on this a bit.

But high-five programs from the Navy and DARPA co-sponsored probably around 80 tests in wind tunnels.

For the Army, about 50 some tests at Mach 10 in a shock tunnel with a hydrogen-based scramjet and 20 at Mach 12.

On the Air Force, roughly 90 tests have been run on—at around the Mach 4–1/2 range going to Mach 6–1/2.

And so this is a point where we have advanced technology and also high-speed turbine technology through to the program have been advanced for a number of years, probably decades, and I believe we are ready to begin the flight demonstration phase of these technologies.



Mr. AKIN. I did not think it was—I did not think the regular—the simple scram and ram jets were turbines. Is there turbines on them?

Dr. SEGA. Yes. In terms of the National Aerospace Initiative, one piece is high speed and hypersonics, hypersonics generally defined at Mach 5 and above, and so the engines themselves generally need about Mach 3–1/2, the scramjets and ram jets do, scramjets in particular, to ignite.

So the question is how do you do that. In the case of high-five, like in a rocket, to bring it up to that velocity, other reusable concepts would have a turbine engine so you would take off as an airplane and accelerate to the right velocity, and then the scramjet can take over, similar to an afterburner.

So I think—

Mr. AKIN. Is that a totally separate engine then, the scramjet, as opposed to the turbine, or is—

Dr. SEGA. Yes, yes. And most concepts are a combined cycle and—concepts are out there, and most that I have seen are separate pro pads for the turbine and the scramjet. But I think it is an important area for us as we advance into the next century.

Speed's important for missile defense, whether a cruise missile or boost to action phase, important for time-critical targets, important for strategic strike options, and it could give us another way of access to space with the first stage being air breathing, the second stage rocket.

And so we have laid out a program that is a stepping-stone approach of—and our target is a Mach number per year, reaching Mach 12 by 2012, but participation from—the services and agencies are all engaged in one place or another in the program. So we are—

Mr. AKIN. Is that a good thing, to have everybody—each agency—or like the Navy's working their program, the Army working something else, is that a good thing, or would it be better to combine it, or is there some logic to have some parallel development when you are kind of in the early development stages?

Dr. SEGA. Well, when I came on board in August, 2001, I saw that there were separate, you know, efforts going on, and the question is are we well integrated, are we well coordinated, and I think, through the last year with the technical community coming together, a series of workshops, and then, after that, building a plan that was vetted with industry to see if we understand where we are technically and what the opportunities are, that we have an integrated plan, and so I think coming at things in a little different ways, as long as it is coordinated and integrated, makes sense.

Mr. AKIN. So each one's learning from the other is—maybe one experiment in one place can help the other.

Dr. SEGA. That is the plan.

Mr. AKIN. Good. Good. Thank you very much. Thank you.

Do I get one extra too?

Mr. SAXTON. Sure.

Mr. AKIN. Okay. Just back on the vaccine area in bio, was this to deal with either bacterial or viral or anything like that, the technology? I came in sort of on the end of that discussion.

Dr. TETHER. Oh, it is really at the DNA level itself. It is—



Mr. AKIN. So it does not really make any difference what the——

Dr. TETHER. No.

Mr. AKIN [continuing]. What the organism is.

Dr. TETHER. Correct.

Mr. AKIN. It could be as small as a virus or some—some big creepy crawlly or whatever it is. You can—you can tailor it to any of these things.

Now does that have tremendous implications in terms of just things like fighting other kinds of viruses, as you said, like colds or AIDS or any of the other——

Dr. TETHER. Well, that is—that is what we are hoping in this program that we have. We do think we—the potential is there for AIDS. The common—if we could get the common cold, we would have—we would not have to worry about these drugs being—I mean the big—the pharmaceutical companies would run with it because it would be a very commercial opportunity, but that is—right now, we have vaccines that will handle—will vaccinate four or five of the major bugs that we are worried about.

Now, when I say that, I mean this is in mice. You know, that is the problem. Okay. We—you know, we have got—there are thousands of drugs that work in mice, that when you go to the next step, you find that they are lethal in humans, you know.

Mr. AKIN. These—are these passive or active vaccines?

Dr. TETHER. Well, they are active. They are——

Mr. AKIN. Active vaccines?

Dr. TETHER. Yes.

Mr. AKIN. Okay. Because I think the—I forgot his name, but the doctor from the Soviet Union that did their bio stuff said that we have to get used to the idea of using an active vaccine——

Dr. TETHER. That is correct.

Mr. AKIN [continuing]. In his opinion.

Dr. TETHER. And—that is correct, and in his techniques——

Mr. AKIN. That is your thought, is the same thing?

Dr. TETHER. Yes.

Mr. AKIN. Well, in that the chairman was—had his attention missing, I will go for one other. [Laughter.]

Mr. SAXTON. Fire away.

Mr. AKIN. The importance of electricity on board our ships. What—is there—how much can you say about where we are with particle as well as laser, and what sort of technologies you are looking—can you use it to defend against incoming kinds of things at this point or——

Admiral COHEN. This is really an exciting area, and you have already heard from the Air Force on the active denial, high-power microwave.

Earlier, I talked about free-electron laser. The Air Force has been working, as you know, on chemical lasers, on the Airborne laser, and that would also be needed in space-based laser.

It turns out that the Navy and the Air Force really have different requirements in this area because the Navy operates at sea level, which is a high atmospheric pressure and, frequently, a hundred percent humidity. We must have a tunable laser frequency. To date, for us, that is the free-electron laser.

Now, when I got involved with this three years ago, we thought the efficiency was 1 percent, but, if you have all electric ship with a hundred megawatts, even if only one megawatt goes out the pointy end, one megawatt per second is one mega jewel. That is one stick of dynamite. So I named that DASL, Dynamite At Speed of Light.

We now find out what the Jefferson Lab is doing with their free-electron laser is 10-percent efficient, and it is about the size of a Tomahawk armored box launcher.

So, on a ship, which is several thousand tons, where we are going to be all electric anyway, and that power can go into the propellers or it can go into radars or it can go into lasers. We see great efficacy for this for close-in defense, anti-air, and downstream potentially ballistic-missile defense in a theater role.

The Air Force has other requirements, and they are pursuing those, and I do not want to speak for the Army or the Air Force, but we do work together under Dr. Sega's leadership here, and, in fact, they are looking at an alternate technology, the solid state high-energy laser which is a similar approach to the free-electron laser, and, just because we are investing, we are finding more lasers are becoming available that are getting smaller, more efficient. DARPA is invested as well.

This is the Wild Wild West, but it is moving very fast, and I believe that we could have this on our ships—DDX is the first all-electric ship—by the end of this decade.

Mr. AKIN. Wow. Thank you.

Admiral COHEN. It changes warfare, in my opinion, as much as Monitor and Merrimac made wooden-hole warships obsolete, but I would like to remind you we continued to build wooden-hole warships for about 40 years—40 years afterwards.

Mr. AKIN. Yes, sir. Thank you.

Thank you, Mr. Chairman.

Mr. SAXTON. Can you—Tony or Admiral, can you define active vaccine for us?

Dr. TETHER. There is one—one vaccine would create antibodies, and that I would call a passive vaccine. The active vaccine goes right after the DNA of the bug that is in there. At least that is my definition of it. That is—I think that is right. I think—that and alive, I guess. Yes. Whatever works.

Mr. SAXTON. Let me back up to the subject that we were discussing for how much of our resources we are spending on the war on terrorism. Tom Hawley and I were with some military folks not long ago, and—it is actually a classified thing, and so I would just be a little bit circumspect—and they were using some information technology to do some pretty amazing things, and we have watched other people use science and technology who are good military folks.

And I am wondering is there—are people who are involved in the war on terrorism accessing your groups and saying we really need to develop the capability to meet this need? Is this a conversation that goes on on a continuing basis, on a daily basis, and do you have the resources available to meet those needs?

Ron.

Dr. SEGA. I will start. I think a few of us have examples to present. The—users—the combatant commanders and the technical community, I think, have come together closer over this last year than I am aware of in any previous time because the situation's so fluid, and the rate of change in technology is so high that—and much of the technology that has been developed in the world is outside of Department of Defense and also accessible to potential adversaries.

And so the need to connect in to the technology community from the war fighter's perspective is high, and I would submit probably going to grow in the future, and so, when we prioritize to the candidate list of technology that I mentioned in the Combating Terrorism Technology Task Force, we would filter it from the—where it was in terms of being able to deliver.

But then we asked for the combatant commands and the Joint Staff working together to prioritize that for us before we made the investment to accelerate it. We used the monies that we—the funds that we had to react to this and, when possible, did some re-programming of funds to meet those needs, but that is also one of the motivations of increasing the Quick Reaction Special Project Fund from the \$25 million requested in 2003 to the president's budget request in 2004 to \$75 million to allow additional current-year flexibility to meet those needs.

Dr. ANDREWS. Maybe I would like to come back to respond to that in two ways. You mentioned earlier that Future Combat Systems is a conventional-like approach. It is not actually. It is a—in the conventional approach, the Army took mass to go solve this problem. We are seeing that today. And how long did it take to get that mass in place? It is still moving to get in place.

What we have done with Future Combat Systems is cut its weight so significantly it can get—that the combatant commanders have asked for—we want—they want the Army forces on the ground somewhere in 96 hours. No force in the world today can do that. If we had it available to us today, you could provide precision attack on those terrorists that were in place in specific parts of the world, Afghanistan, wherever it may be.

So Future Combat Systems is one of their priorities for the war on terrorism, and it is a different way. It is really unprecedented in knowledge, speed, and precision across the full spectrum of conflict. Our main—heavy forces today cannot go after that kind of terrorist.

Mr. SAXTON. Could I—go ahead. I will come back to that.

Mr. ENGLE. I guess just, Mr. Chairman, to address your question of exchange of information between presumably, in my case, warfighter and me the producer of science and technology, I would take you back to our Battlefield Air Operations Kit.

That was actually communicated directly to Secretary Roche as he was pinning the Purple Heart on Staff Sergeant Yoshida, and the secretary turned to him and said, young man, what else can we do to make your job easier, and he says, well, sir, my job is to use the information I provide to combat terrorism to close the kill chain between, you know, the platform and the bullet and the terrorist, and I have got this basic problem, 150 pounds on my back.

So, in very short order, almost in real time, the attention to the lab returned on that particular problem, as I mentioned in my testimony. That is happening almost routinely right now as we speak in many areas in the Air Force and I am sure in the other services between those that are in the field finding new problems that they are having difficulty solving and bringing them forward to the laboratory and to the product centers to try to get something, you know, in the field as rapidly as possible.

And I think we are doing a pretty good job in responding to that as the ideas come in and time and technology can accelerate within the realm of reason.

Mr. SAXTON. With regard to the subject that I was discussing with you before, the—are there technologies—I continually see things that amaze me, and the use of technology in different ways is absolutely astounding to me.

And I am wondering are there—are there programs that you are involved in and—in any of your agencies that are—that are going—that have the potential to help us in the—in significant ways in intelligence information gathering?

Admiral COHEN. Mr. Chairman, as you are aware, in the Navy, we went away from the Advance Technology Demonstrators three years ago because we would provide wonderful, workable devices, but, because of the limited resources in acquisition, the—although they were highly desired, they were ahead of their time, and there were not the resources to invest to transition them and go into acquisition.

So, in the future Naval capabilities, I now invest precious 63 only when somebody dealing like Dr.—with Dr. Tether—they have a written memorandum of understanding and hard money put down in the acquisition side. It is programmed over the FYDP.

I am investing more than \$70 million a year in what we call knowledge superiority and insurance. It is one of our FNCs. It goes directly at what you are addressing, Mr. Chairman.

Now we focus primarily on netcentric warfare, which brings together all of the space, air, surface, and subsurface sensors so that we can then complete the kill chain, but when you are able to do that and you have the bandwidth and you have the protocols and you have the manned machine interface, its application across anti-terrorism is a small step to take.

So it may have something quiet in this area because the war on terrorism is just one component of the war that we are required to be prepared for and conduct as we are now.

Mr. SAXTON. You bet, but let me just—let me just make a comment on that. And I think this is really important.

Ten years—12 years ago, we showed the world that Saddam Hussein could not compete with us. We are showing him again now. Twelve years ago or 11 years ago, the Soviet Union collapsed, and I do not think it—that—except for maybe the nuclear threat, I do not think anybody would claim that, with their capability and readiness today, they can compete with us.

So there is—we have essentially shown the world that, if you want to get at the West or the United States, you cannot do it with conventional forces. And, therefore, we have seen over the last 12



years, an emergence of a significant threat that did not exist at least to the point that it does today.

And so when we—we have seen—it is—my opinion is that we continue to emphasize the development of conventional capability, which is fine, because we have to think about tomorrow as well as today. But we have some threats that exist today that we cannot manage, and that is why I get excited about—about these things.

Dr. TETHER. We have—we have some programs that probably are more—closer to what you would like to hear about, but I—this is not the place to hear about it.

Mr. SAXTON. This is not the place to do it. That is right.

Dr. TETHER. And Jean will be over, and we will get—we will dunk his head in the pocket, but there are programs. Amazingly enough, the programs are not necessarily large dollars, but—

Mr. SAXTON. Jean and I were just talking earlier, Secretary Andrews, about having a—a future weapon—a Future Combat Systems hearing later after we get past our busy season here marking up and what have you. But I just have—when you were talking about FCS before, you mentioned 20 tons. Is that per vehicle?

Dr. ANDREWS. Future Combat Systems is comprised of about 18 systems right now, about half of them manned, half of them unmanned. The largest vehicles are about 20 tons, and what we are looking for is a family of systems that you can get commonality in the structure. The unmanned system is going to be somewhat less than that weight typically. The six-ton vehicle you saw up here probably is max high.

So what Future Combat Systems does for us is allow us to—when we are getting—when we are sent somewhere, you are now taking a larger effective force in a lot less space and weight, and yet more of the power of the network comes with you, as well as lethality and survivability.

Mr. SAXTON. Understand. And Boeing came in the other day with some nice charts and showed me how much of the—we had a great briefing. Here is what I want to say to you.

Dr. ANDREWS. Yes, sir.

Mr. SAXTON. Because of—somehow in the processes developed in the Striker, which is also 20 tons, somebody decided that we were going to deploy these systems in 96 hours, just like you said, and, with the deployment equipment, i.e. airplanes, that we have available today, you have to use C-130's.

Dr. ANDREWS. Yes.

Mr. SAXTON. Well, guess what. The Striker's too heavy. It weighs 40,000 pounds, maybe more than that with the crew and ammo and crew equipment, and—I will tell you this story because I do not want to see this happen to the Future Combat System because it—it is a—it is not very nice.

I heard that it would not fit in the C-130. Well, people told me, it will fit in the C-130. Do not worry about it, Congressman. As a matter of fact, we are going to fly three up to McGuire Air Force Base on a C-17, and we will show you that it fits in a C-130.

So the Army did that. They brought three up on a—flew them in on a C-17, which I should have—I should have figured something out when I saw the C—when I heard about the C-17, but I did not get it right away, and, sure enough, they put one up, and



they put a ramp of a C-130 down. They drove it up in there. They chained it down. It was neat. It had four inches on each side and 18 inches over the top. Needed a waiver to fly it that way, but that is Okay. And I said, hey, you guys are right, it fits.

So, while I was there, General Williams, who is commander of AMC, said would you like to talk to the crew. I said sure. So we went up to the cockpit, and we are talking to the crew. I said do you always fly with 40,000 pounds. Oh, almost never, sir. I said, well, how far can you fly. He said, well, depending on climate, depending on altitude, sometimes to a location a couple hundred miles away. But, on a bad day, maybe as little as 60. I said you are kidding.

Now, when we were in conference marking up and—I think the Senate had included funding for the Striker and the House did not, and so Chairman Hunter got a call from the Army leadership saying we have got to have this system because we have got to have a system we can deploy on C-130's and be in the fight in 96 hours. Well, the Striker ain't going to do that. It is too heavy.

So, in planning this family of vehicles, please go see the Air Mobility Command and say how many C-17s can we use for this mission and how many—and how heavy can we be to deploy in C-130's from reasonable locations for reasonable distances to get to the fight in 96 hours.

Dr. ANDREWS. We are pushing very hard to keep it down around 16 tons, in this case—

Mr. SAXTON. Well—

Dr. ANDREWS [continuing]. Which is closer to when you go off and fly and the range you need because, once we get there in C-17s, then we will be deployed by C-130's which may be a few hundred miles at the most.

Mr. SAXTON. Okay. Right. If we were—if we were deploying into Iraq today, it would be marginal with a 40,000-pound load. I am not sure you could do that. You would have to fly—well, you would fly it in the C-17 to a point—

Dr. ANDREWS. Like the air base we just took over possibly.

Mr. SAXTON. Yes, right. And that is fine. But to have a capability of flying to a location 60 miles away is not fine. Wouldn't you agree?

Dr. ANDREWS. I am not a war fighter, but it would not seem necessarily logical, but—

Mr. SAXTON. You may—that is where you may need the forces right then. So AMC made me some charts based on deployment into Afghanistan, and, at 38,000 pounds, from six airports in the Afghan theater, because of altitude, at six of the airports, the C-130 could not take off with 40,000 pounds on the board.

Well, I guess it was 38,000 pounds. I have forgotten exactly. I have forgotten the charts, but it was very discouraging to see the number of airports in the Afghan theater that the C-130 could not take off with 38,000 and 40,000 pounds on two charts, two different examples. So—

Dr. ANDREWS. And the challenge is we are—essentially, that becomes an asymmetric threat against us, and so, until we take on that problem of reducing our weight, we are going to be helped to certain places we cannot go.

Mr. SAXTON. I agree.

Dr. ANDREWS. So I—you know, it is at 16 tons or better kind—around that kind of number.

Mr. SAXTON. Now let me bring up one other subject. And I am sorry for—I—this is not the—really the place to talk about this, but we are engaged in these things, so—and I am just—

Dr. ANDREWS. And I am just a technology guy. I am not—

Mr. SAXTON. We are—we—the Army's Special Metals Division—that is not the right title.

Dr. ANDREWS. The Nay Labs.

Mr. SAXTON. It is up at Aberdeen. Called Special Metals; has developed a theory to refine titanium domestically and cut the cost of it by at least half, and we need to pay special attention to this. I have heard about—they are taking it from the—\$20 a pound or so down to probably about \$3 or \$4, and I have got a briefing on its way.

Dr. TETHER. Down around \$5.

Mr. SAXTON. Five then. Now that would mean a lot to you.

Dr. TETHER. Oh, yes. Yes, we buy a lot of it.

Mr. SAXTON. You bet. You bet. And this 38,000-, 48,000—40,000-pound weapons system would be a different animal, wouldn't it?

Dr. TETHER. You are right.

Mr. SAXTON. Okay. We will work together.

Dr. TETHER. Yes, sir. And we have a major DARPA program in getting titanium down. Not—it is not just titanium. It is in the alloys. I mean you really want to end up with titanium alloy, and we will be happy to share that with you.

Mr. SAXTON. Hey, thank you. You are all doing great work. I do not know if either of my other colleagues want to ask another question, but we have been here for a couple of hours, and it is 6:30, and it is probably time to go home, but—

Dr. TETHER. Well, thank you.

Mr. SAXTON. Yes. Thanks—thanks a lot for the great work you do. We really appreciate it, and, as I said in my opening statement, we are where we are today with national security because of advances in technology. That is where you are, and we appreciate it, and we want to do what we can to help you. Thank you.

[Whereupon, at 6:20 p.m., the subcommittee was adjourned.]



---

# **A P P E N D I X**

MARCH 27, 2003

---





---

---

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

**MARCH 27, 2003**

---

---



Opening Statement of Congressman Jim Saxton  
Chairman, Subcommittee on Terrorism, Unconventional Threats and Capabilities  
House Armed Services Committee

Hearing on Defense Science and Technology for Future Force Capabilities – The  
War on Terrorism, Transformation, and Beyond  
March 27, 2003

Today, the Subcommittee on Terrorism, Unconventional Threats and Capabilities will hear testimony on the status of the Department of Defense science and technology program and plans and priorities for the future. We will discuss with Director of Defense Research and Engineering Ron Sega, the military departments' science and technology chiefs, and the Director, Defense Advanced Research Projects Agency some of the issues faced by the program today, how the program has been reshaped to support the War on Terrorism and support to our forces in Iraq, and what needs to be done to accelerate the identification, development, and transition of advanced technologies we will need to ensure the superiority of our armed forces on the 21<sup>st</sup> Century battlefield.

In 1983, then Secretary of Defense Caspar Weinberger said:

"We face the danger of losing our edge because we have not adequately replenished the reservoir of scientific concepts and knowledge to nourish future technologies during subsequent years of fiscal neglect of defense research and development. Given these circumstances, we must systematically replenish the scientific reservoir, using the unique and diverse strength of the United States scientific community ... Given the relatively long lead time between fundamental discovery and applying such knowledge to defense systems, the true measure of our success ... may not be apparent for several decades. When the 'moment of truth' arrives, we cannot afford to be found wanting. Thus we must revitalize the productive partnership between the university community, industry, and the DOD in-house laboratories."

Technological superiority over our adversaries is a cornerstone of the U.S. national military strategy. Historically, a robust Defense science and technology program has been key to meeting the known needs for military capabilities, providing a technology bridge to new weapons systems during periods of reduced funding for development and acquisition, and enabling the development of totally new operational concepts and capabilities. The combat capabilities that overwhelmed the Iraqi Army in Operation Desert Storm in 1991 were the result of technology investments made in the 1950's and 60's that matured into development and acquisition programs in the 70's and 80's. Advances in semiconductor technology and information technology in the 70's and 80's are at the heart of the weapons systems and command and control that are the focus of the precision strike capabilities being used in Iraq today. Basic and applied research in areas such as nanotechnology, robotics, wide band gap semiconductors, and the

biological revolution will lead to advanced radar and weapons systems in the future and to other capabilities for our armed forces that are as yet unforeseen.

For the past two decades, both before and after the end of the Cold War, previous Administrations and the Congress have faced the issues raised in Secretary Weinberger's 1983 statement regarding the Defense science and technology program. These issues confront the Bush Administration and the Congress today: what should be the role of the federal government and the Department of Defense in supporting science and technology research and development; on what technologies should the Defense S&T program focus; what is the appropriate level of funding for the program; what is the best process for planning and managing the program; what is the relevance of the DOD laboratories to the program and what is needed to support an aging Defense Department laboratory infrastructure; what is needed to ensure a continuing supply of competent engineers and scientists for Defense research and acquisition; how do we accelerate the transition of technology from the laboratory to the military user in the field; and, how are we changing the program to support the War on Terrorism and the other threats that confront our nation.

To address these issues we have a distinguished panel of witnesses from the Department of Defense:

The Honorable Ronald M. Sega  
Director, Defense Research and Engineering

Dr. A. Michael Andrews  
Deputy Assistant Secretary of the Army for Research and Technology

Rear Admiral Jay M. Cohen  
Chief of Naval Research

Mr. James B. Engle  
Deputy Assistant Secretary of the Air Force (Science, Technology and Engineering)

Dr. Anthony J. Tether  
Director, Defense Advanced Research Projects Agency

Gentlemen, we welcome you and look forward to your testimony.

Dr. Sega, before you begin, I'd like to yield to the Ranking Member of the Subcommittee, Congressman Marty Meehan from Massachusetts.

Mr. Meehan

**FOR OFFICIAL USE ONLY  
UNTIL RELEASED BY THE  
HOUSE ARMED  
SERVICES COMMITTEE**

**TESTIMONY OF**

**RONALD SEGA**

**DIRECTOR OF DEFENSE RESEARCH AND ENGINEERING**

**BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES**

**COMMITTEE ON ARMED SERVICES**

**SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS  
AND CAPABILITIES**

**March 27, 2003**

**FOR OFFICIAL USE ONLY  
UNTIL RELEASED BY THE  
HOUSE ARMED  
SERVICES COMMITTEE**



## Introduction

Mr. Chairman, members of the committee, thank you for the opportunity to appear before you today to talk about transformation and the Science and Technology (S&T) program of the Department of Defense. I appear before you today with excitement about the capabilities and possibilities being opened by science and technology throughout the Department of Defense. Before addressing specific aspects of the Defense Department Research and Engineering (R&E) program, let us recall the pledge made by President Bush upon taking office. The President said that he would order "an immediate, comprehensive review of our military—the structure of its forces, the state of its strategy, the priorities of its procurement." He also said his goal would be "to move beyond marginal improvements—to replace existing programs with new technologies and strategies." The President made technology one of the cornerstones of his mandate to transform defense. Now that we are two years into President Bush's administration, I believe it is a good time to review how well the DoD S&T program is enabling transformation. I will highlight some recent accomplishments and the planned direction of the S&T program.

As the Director of Defense Research and Engineering, functioning in the role of the Department's Chief Technology Officer, I have established five goals. These five goals are consistent with, and derived from the goals and objectives

laid out by the Under Secretary for Acquisition, Technology, and Logistics, Mr. Pete Aldridge. The Research and Engineering goals are:

- Integrate DoD S&T and focus on transformation
- Enhance technology transition
- Address the national security science and engineering workforce
- Expand outreach to the combatant commanders and intelligence community
- Accelerate support to the war on terrorism

Taken together, they provide a sound strategic R&E framework to support transformation in the Department of Defense. I will address each of these five goals separately—and in so doing, will thereby describe the direction of the overall S&T program.

#### Integrate DoD S&T and Focus on Transformation

There are two key elements to this goal—*how much* the DoD invests in S&T, and *what technologies* the Department invests its S&T dollars.

The FY04 President's Budget Request is a good budget request for science and technology. The DoD request for S&T in FY04 is \$10.232 Billion, or 2.69% of the overall Department of Defense request. The budget request achieves greater than zero percent real growth for S&T, when compared to the combined FY03 President's Budget Request and Disaster Emergency Relief Fund. Significant

overall growth in S&T investment has occurred since the budget request of \$7.8B in FY 02. This is a budget increase for S&T of nearly 25% in just two years.

However, simply adding money to the S&T accounts will not ensure transformation. We have also focused the budget request on several important technologies that should enhance transformation and deliver superior military capabilities. Last fall, we decomposed the entire S&T budget, and found that nearly all S&T dollars are aligned to support Secretary Rumsfeld's six critical operational capabilities as outlined in the Quadrennial Defense Review. These capabilities are: protect bases of operations, deny enemy sanctuary, project and sustain US forces, enhance space operations, assure information operations, and leverage information technologies. The DoD S&T investment request is aligned to develop technology that should directly enhance these capabilities.

Additionally, we identified three broad, cross cutting initiatives that address the development of DoD critical transformational technologies. The three areas are the National Aerospace Initiative; Energy and Power Technologies, and Surveillance and Knowledge Systems.

The Services are investing in these areas and other high profile transformational projects. The Army Future Combat System is a transformational project that combines combat and support vehicles and unmanned air and ground systems that will work together as an integrated system-of-systems. The Army's Objective Force Warrior will decrease the equipment weight of the deployed infantry soldier from around 100 pounds to 40 pounds. The Air Force is

developing enhanced precision weapons and directed energy weapons that will provide a battlefield commander greater options to deal with a threat with graduated effects. The Navy is moving to an electric force, with advanced propulsion concepts and electric weapons.

In addition, we have increased our investment in the Defense Research Advanced Research Agency (DARPA) by almost a half billion dollars a year with a significant additional investment allocated to space technology. DARPA continues to emphasize high-risk, high payoff research in a number of strategic thrust areas, as outlined in the DARPA Strategic Plan. I would like to highlight a DARPA project that is supporting transformation in the Department with Service collaboration. The Organic Air Vehicle (OAV) is a small, man-portable unmanned aerial vehicle (UAV) that can fly and hover in a battlefield using a large horizontal fan for moving and hovering. The UAV has been tested in 9, 15, and 29 inch diameter version—and each can carry different payloads. This “system” is being developed as a component of the Army’s Future Combat System. DARPA’s programmatic agility, when linked with Service programs, accelerates technology development and transformation.

In addition, we have increased the investment in demonstrations, primarily through Advanced Concept Technology Demonstrations (ACTD) over the past two years, from \$150M in FY02 to over \$213M in FY04. The ACTD program was instrumental in demonstrating the utility of UAVs such as the Global Hawk and Predator. The ACTD program harvests the technology developed in the

Defense laboratories and industry, and integrates these technologies into demonstrations that provide a glimpse into the future. I will highlight two of the more than 70 ACTD projects currently underway to give you a feel of the breadth of these efforts. The Language and Speech Exploitation Resources, known as LASER ACTD is a software package used to read or hear foreign text and translate the language into English. This system translates Arabic, Farsi, Pashtun, as well as numerous other languages, and is in operational use in both Afghanistan and Iraq. The Active Denial Technology ACTD is demonstrating the ability of high power microwave systems to prevent unwanted access to installations—in effect, giving the military commander a non-lethal option to protect an area. We have also increased our investment in experimentation, primarily joint experimentation, and are executing this investment through Joint Forces Command. This new investment lets the Department conduct large and small scale “experiments” or war games to effectively “try technology before it is bought.”

One of the joint transformational technology initiatives is the National Aerospace Initiative (NAI), which consists of research and development in hypersonic flight technology, affordable and responsive space launch, and enhanced on-orbit space technologies. In the FY04 budget request, the Department focused the increased investment into hypersonic technology, investing over \$150M additional funds in hypersonics. We seek Congressional support for the FY04 budget request for the increased hypersonic technology work



and the integrated technologies of NAI. Hypersonic technology could be truly transformative as it could provide increased capability through speed in several mission areas. For example, hypersonics could provide the opportunity to conduct tactical strikes from strategic distance in a short amount of time. Technology has progressed to the point where we believe that demonstrations of a Mach number per year, reaching Mach 12 by 2012, are within reach. The development of hypersonic technology could reduce vulnerability of future systems, while potentially providing a flexible capability to strike quickly and effectively deny enemy sanctuary anywhere in the world. Additionally, a hypersonic roadmap, developed cooperatively by DoD and NASA provides long term potential for affordable access to space. In short, the National Aerospace Initiative is one of those technology opportunities that has the potential to capture American interest in technology, much like the race to the moon in the 1960's, while providing needed technical capability for the warfighter. The National Aerospace Initiative is the right initiative for America as we celebrate the first century of manned flight

A second transformational technology thrust is Energy and Power Technologies. It involves a coordinated investment by all three Services and DARPA to generate, store and use power in systems ranging from microsystems to future generation electric ships. This initiative is investing in technology that could develop batteries with over five times the energy density, fuel cells that are reliable and safe to use in the battlefield, and capacitors that will decrease size needed to store electricity on ships by a factor of 5-10. This effort could also

potentially impact military operations logistics tail to provide efficient energy and electrical power to forces and systems. In short, this thrust could also truly transform the military.

The final cross cutting initiative is Surveillance and Knowledge Systems. This initiative will seek to develop low cost sensors with various capabilities (such as optical, IR, acoustic, magnetic, biological, chemical, and so forth), connect these information sources to tactical networks, route the data from tactical to strategic level, and finally, the initiative will develop technologies that can assist the decision-maker. The initiative should continue to make the vision of network centric warfare a reality. Taken together, the FY04 President's Budget Request for S&T represents a budget that continues to develop the technologies the US military will need into the 21<sup>st</sup> Century.

#### Enhance Technology Transition

The Department is streamlining the acquisition process built around spiral development and evolutionary acquisition. The key element of spiral development and evolutionary acquisition is a process that allows the Department of Defense to field ever increasing capabilities brought about by enhanced technology without having to initiate a new acquisition program. This is a capabilities-based approach, and is consistent with Secretary Rumsfeld's mandate to transform the DoD capabilities.

To enhance technology transition, we need to provide the means and incentives to programs that accept the new technology. The Department is testing three pilot projects contained in the Quick Reaction Special Program (QRSP). I was pleased that the FY 03 Authorization Act supported the QRSP. Three QRSP projects are complementary and focus on developing technology at different maturity levels. These three projects are the Defense Acquisition Challenge Program, the Technology Transition Program, and the Quick Reaction Fund. All three require vetting by the acquisition, technology and warfighting community, but can fund specific activities within the execution year. The Quick Reaction Fund, initiated in FY03, is already developing technology that could be used in current operations and is modeled after the success of the FY02 Quick Reaction Munitions Fund.

In the FY 02 appropriations bill for the Defense Emergency Relief Fund, Congress identified \$15 million for the Quick Reaction Munitions Fund. Two successful projects resulted from the funding. The first was the Thermobaric Hellfire Enhanced Capability that increased blast lethality in enclosed structures from the hellfire missile. Within one year, the project went from chemistry to the field at a cost of \$13 million. The Low-Cost Guided Imaging Rocket (LOGIR) was the second project. It is enhancing the accuracy of the unguided 2.75" "hydra" rocket used in close air to ground operations. The type of outcome we achieved from the Quick Reactions Munitions Fund should occur through use of the Quick Reaction Special Projects—and should effect technology transition.

We believe the potential payoff from the QRSP is very large—and have consequently added \$50M more in the FY04 budget request compared to FY03. The request for QRSP in FY 04 PBR is \$75M. We seek continued Congressional support in the program, and seek your help in ensuring there is sufficient flexibility in the program to allow the DoD to effectively move rapidly to meet the needs of the Department. We request the QRSP program not be further divided or earmarked, so we can have the freedom to manage and effectively support rapidly evolving technologies and new needs from the warfighter.

#### Address the National Security Science and Engineering Workforce

The third DDR&E goal is a broad strategic national issue involving the availability of scientists and engineers who are American citizens. One can argue that the US national security advantage over the past half century was fueled by the production of scientists and engineers—America has had the intellectual capital advantage. There are signs that America's advantage is eroding. The number of the scientists and engineers ultimately performing work for the Department of Defense draws from the pool of quality U.S. scientists and engineers. One could argue that the national defense engine of the end of the twentieth century was in part fueled by the increase in scientists and engineers produced in the US after the launch of Sputnik and the cold war. There was an excitement about science that resulted in an ample supply of scientists and engineers that would work on national security issues. The United States was able

to produce stealth, the global positioning system, night vision devices, and precision weapons by this pool of scientists and engineers. The Department of Defense pioneered the development of the internet through the "ARPANET". The large capacity of scientists produced the technologies leading to the superior military capabilities today. We believe it is time to rekindle the excitement of science and engineering as a national asset.

The FY04 President's Budget Request for Basic Research is \$1.3B dollars, of which over 50% goes directly to universities. We estimate that every \$1M of university graduate student research supports between 10-15 graduate students, who work in areas of interest to the Department.

#### Expand Outreach to the Combatant Commanders and Intelligence Community

We are enhancing the connectivity between the Combatant Commands and the Intelligence Community and the DoD technology community. We have identified a specific individual to interface with each of the combatant commander's on technology issues. The intent is to enhance coordination so that we can reduce technology surprise by potential adversaries and increase technology options for our warfighters. This outreach extends to other interagency groups.



### Accelerate Support to the War on Terrorism

This is our most important near term goal. Within a week of the attacks of September 11, 2001, the Department established the "DoD Combating Terrorism Technology Task Force". This Task Force is still on-going, and meets as needed to address specific technology opportunities and or needs. The Task Force is comprised of executive level technology members from all DoD Components, flag-level officers from the Joint Staff and selected Combatant Commanders, the Central Intelligence Agency, the Department of Energy, and now the Department of Homeland Security.

Early efforts in the Fall of 2001 resulted in such capabilities as: the GBU-118B (thermobaric weapon) with applications to caves and tunnels, a backscatter gamma ray system to inspect cargo without going into the container, and a nuclear quadripole resonance system that can detect small quantities of explosives. The thermobaric weapon was matured from basic chemistry to a fielded system in 90 days. We also sponsored a rapid study to determine radiation levels needed to kill anthrax spores—knowledge that helped the postal service in late 2001.

Recently, the DoD Combating Terrorism Technology Task Force's focus has been on technologies to detect and "neutralize" chemical and biological agents. The Task Force has worked primarily with the United States Central Command and Special Operations Command. Specific details are still classified, but may be provided in an appropriate forum.

The continued investment in science and technology over the past decades enabled the Department's development of these needed new capabilities. I believe this is very important for developing technology and transformation. Good technology development is largely achieved through long-term, stable investment in science and technology. Not every technology needs to be transitioned immediately but a strong S&T base is critical. The FY04 President's Budget does focus on transformation technologies. But it also maintains long-term technology based investment in such capability areas as materials and nanotechnology, electronics, sensors, and so forth. The balance has been, and remains important.

In closing, the science and technology program and the objective of Secretary Rumsfeld to provide transformational capabilities to the DoD are absolutely intertwined. I have mentioned only a few examples within the DoD S&T program. I believe the Department of Defense successes in technology and transformation are significant, and I appreciate the opportunity to come before you today to tell you about them. Thank you.

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE

**Statement by**

**Dr. Tony Tether**

**Director  
Defense Advanced Research Projects Agency**

**Submitted to the**

**Subcommittee on Terrorism, Unconventional Threats and Capabilities  
House Armed Services Committee  
United States House of Representatives**

**March 27, 2003**

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE

Mr. Chairman, Subcommittee Members and staff: I am very pleased to appear before you today to discuss the Defense Advanced Research Projects Agency's (DARPA) Fiscal Year (FY) 2003 activities and our FY 2004 plans to continue to transform our military through technological superiority.

Let me begin by saying a few words about the DARPA.

Since the time of Sputnik, DARPA has had a special mission within the Department of Defense (DoD). Our mission is to maintain the technological superiority of the U.S. military and prevent technological surprise from harming our national security. DARPA does this by sponsoring revolutionary, high-payoff research that bridges the gap between fundamental discoveries and their military uses.

DARPA prevents technological surprise by filling that gap long before our adversaries can, and, at its very best, DARPA also *creates* technological surprise for our adversaries. An example is DARPA's development of stealth – a dramatic technological capability that continues to put our adversaries at a disadvantage.

DARPA fulfills a unique role within the DoD. As a Defense Agency, DARPA reports to the Secretary of Defense and is the Secretary's only research agency not tied to a specific operational mission. DARPA is designed to be the "technological engine" for transforming the DoD, supplying technological options for the entire Department.

This is a unique role within DoD. The Department's operational components focus on nearer term needs at the expense of long-term change because of their emphasis on near-term urgent needs and requirements. Consequently, a large organization like the DoD needs an organization like DARPA whose *only* charter is radical innovation. We try to imagine what a military commander would want in the future and accelerate that future into reality by changing people's minds about what is technologically possible.

### **DARPA's Eight Strategic Thrusts**

Through the years, DARPA has continuously refocused its work in direct response to evolving national security threats and to technological opportunities. DARPA's *Strategic Plan*, which describes how we are pursuing our mission through today's changing circumstances, was submitted to Congress on February 3, 2003.

That report details the eight strategic research thrusts that DARPA is emphasizing today:

- Counterterrorism
- Assured Use of Space
- Networked Manned and Unmanned Systems
- Robust, Self-Forming Networks
- Detect, Identify, Track, and Destroy Elusive Surface Targets
- Characterization of Underground Structures
- Bio-Revolution
- Cognitive Computing

I want to tell you about these eight thrusts, the forces driving them, and illustrate them with some example programs.

#### Counterterrorism

Foremost in our minds today is protecting Americans against acts of terror and the networks that perpetrate them. DARPA's counterterrorism strategic thrust has two major elements: Information Awareness and Biological Warfare Defense.

The goal of our Information Awareness programs is to create information technology that America's national security community can use to detect and defeat terrorist networks before they can attack us.

This work has been greatly expanded as a direct result of the September 11th attacks. It includes research in technologies to identify people at a distance, translate written and spoken languages into English, vastly increase the size and searchability of databases, improve decision-making by policy makers, find patterns in scattered data, and predict the behavior of terrorist groups.



One of our Information Awareness programs is Total Information Awareness (TIA), around which there has been much controversy. If I knew only what I read in the press about TIA, I would be concerned too. So I'd like to briefly address some of the main concerns.

No American's privacy has changed in any way as a result of DARPA's Information Awareness programs, including TIA. The Department of Defense *is not* developing technology so it can maintain dossiers on every American citizen. The Department of Defense *is not* assembling a giant database on Americans.

Instead, the TIA program is designed as an experimental, multi-agency prototype network that participating agencies can use to better share, analyze, understand, and make decisions based on whatever data to which they currently have *legal* access. TIA will integrate three broad categories of information technologies from DARPA and elsewhere: advanced collaboration and decision support tools, language translation, and data search and pattern recognition.

The ultimate goal is an interagency network to collaborate, "connect the dots," and prevent terrorist attacks. While the research to date is promising, TIA is, today, a series of experiments. We want to be clear that the DARPA program is an R&D project only. The Omnibus Appropriations Act of Fiscal Year 2003 (P.L. 108-007) requires that before we make major investments in preparation for deployment of a working system, we will need to make our case for deployment and Congress must permit such deployment.

TIA is a program to make new tools. It does not permit any agency access to data that they don't already have, and it in no way alters the authority or responsibilities of those agencies in that regard. Policymakers, particularly Congress, will ultimately determine how TIA tools may be used and on what data.

On February 7, 2003, the DoD announced the establishment of two boards to oversee TIA. These boards, an internal oversight board and an outside advisory committee, will work with DARPA as we continue our research. They will help ensure that TIA develops and disseminates its tools to track terrorists in a manner consistent with U.S. constitutional law, U.S. statutory law, and American values.

In late February, we had our first meeting with the internal board, chaired by the Under Secretary of Defense (Acquisition, Technology and Logistics). We look forward to working closely with both oversight boards as we continue our work on TIA.

The second element of DARPA's counterterrorism strategic thrust is Biological Warfare Defense (BWD). DARPA's BWD program began in the mid-1990s in response to a growing awareness that changes in the strategic and technological environment had sharply increased the biological warfare threat to the United States.

DARPA's BWD program is comprehensive and aggressive. It covers sensors to detect an attack, technologies to protect people in buildings and manage the response to an attack, vaccines to prevent infection, therapies to treat those exposed, and decontamination technologies to recover the use of an area. I discussed our work in this area in some detail in testimony before this subcommittee on March 19th, so I won't repeat that today.

#### Assured Use of Space

The national security community, generally, and the U.S. military in particular, use space to provide warning, intelligence, communications, and navigation. These orbiting assets are one of the great advantages the U.S. military has over potential adversaries. And American society relies on space for everything from communications to weather reporting, making space assets a vital element of the U.S. economy and our way of life.

This military advantage and civil dependency have not gone unnoticed by our adversaries, and there is no reason to believe that they will remain unchallenged or untested forever. When I became the Director of DARPA, the Secretary of Defense directed DARPA to begin an aggressive effort to ensure that the U.S. military retains its preeminence in space by maintaining unhindered U.S. access to space and protecting U.S. space assets from attack.

There are five elements in DARPA's space strategic thrust:

- *Access and Infrastructure:* technology to provide rapid and affordable access to space
- *Situational Awareness:* the means for knowing what else is in space and what that "something else" is doing
- *Space Mission Protection:* methods for protecting U.S. space assets from harm

- *Space Mission Denial:* technologies that will prevent our adversaries from using space to harm the United States or its allies
- *Space-Based Engagement:* technologies for space-based sensing, communications, and navigation to support military operations on earth

Four examples of DARPA's space programs are Responsive Access, Small Cargo, Affordable Launch (RASCAL); Space Surveillance Telescope; Orbital Express; and Innovative Space-Based Antenna Technology.

RASCAL is designed to place small payloads in orbit on a moment's notice by launching them from a high-speed, high-altitude, reusable aircraft that eliminates a large and expensive first stage booster. RASCAL is aimed toward a system to place 50- to 130-kilogram satellites and commodity payloads into low earth orbit at any time, at any inclination, and with a launch cost that is less than a third of current capabilities for the dedicated micropayload size.

The Space Surveillance Telescope program is developing a ground-based, wide-aperture, deep field-of-view optical telescope to search for very faint objects in geosynchronous orbit. It will enable us to identify and assess unidentified objects that suddenly appear in orbit with unknown purpose.

Orbital Express will demonstrate the feasibility of using automated spacecraft to refuel, upgrade, and extend the life of on-orbit spacecraft. It will lower the cost of doing business in space and will provide radical new capabilities for military spacecraft, such as high maneuverability to make our satellites more difficult to track and evade, autonomous orbital operations, and satellites that can be reconfigured as missions change or as technology advances. Orbital Express just announced a launch date of March 2006, and we look forward to updating you on our progress in the coming years.

The Innovative Space-based Antenna Technology (ISAT) program is developing revolutionary large antenna technologies that could one day enable large, yet affordable, space-based radar (SBR) systems capable of operating at medium earth orbit (MEO). MEO-based SBR enables persistent, continuous coverage of ground mobile targets with far fewer satellites than that required with constellations based in low earth orbit.

ISAT successfully completed its Phase I feasibility study. Contractors completed mechanical testing on critical, lightweight, space-qualified structures that enable over 100 to one volumetric compression for stowing large antennas for launch. Phase II just commenced and focuses on additional antenna structures testing and detailed designs for a space-based demonstration, with a planned launch in 2009.

#### Networked Manned and Unmanned Systems

DARPA is working with the Army, Navy, and Air Force toward a vision of filling the battlespace with unmanned systems that are networked with manned systems. Improved processors and software have enabled the major increases in onboard processing needed for unmanned systems to handle ever more complex missions in ever more complicated environments.

The idea is not simply to replace people with machines, but to team people with robots to create a more capable, agile, and cost-effective force that lowers the risk of U.S. casualties. There is an increasing appreciation within the Services that combining unmanned and manned systems can enable new combat capabilities or new ways to perform hazardous missions. The use of unmanned air vehicles (UAVs) in Afghanistan began to demonstrate the potential of this idea.

A prominent program in this area is Future Combat Systems (FCS), which DARPA is conducting with the Army. FCS is catalyzing the Army's transformation to the Objective Force, an aggressive and far-reaching program that will profoundly change how the Army fights, trains, equips, and sustains 21st century operations. FCS is a networked system of systems that includes advanced manned combat vehicles as well as unmanned ground and air systems. The goal is to develop brigade-sized formations called "Units of Action" that have the lethality and survivability of an armored, heavy force, the deployability of an airborne force, and the tactical agility of an air-assault force.

DARPA has been at the forefront of the aggressive FCS initiative. We are conducting demonstrations of advanced prototypes, including unmanned ground reconnaissance and attack platforms; low-cost tactical precision munitions; small UAVs that support operations in urban and mountainous environments; and sensors that can detect vehicles camouflaged under dense foliage. A Defense Acquisition Board scheduled for May could allow FCS to enter System

Development and Demonstration under Army management this year. This will enable the Army to field an FCS Unit for operational testing in FY 2008, with the first Unit of Action ready for operational deployment by 2010.

DARPA is also conducting three unmanned air combatant programs: the Unmanned Combat Air Vehicle (UCAV) with the Air Force, UCAV-N with the Navy, and the Unmanned Combat Armed Rotorcraft program with the Army. These aircraft will be teamed with manned systems on the ground and in the air to transform how the Air Force suppresses enemy air defenses, how the Navy suppresses enemy air defenses and conducts extended surveillance, and how the Army conducts armed reconnaissance and attack.

The UCAV program has been conducting flight demonstrations with two X-45A demonstrators at NASA Dryden Flight Research Center at Edwards Air Force Base in California. The first block of flight demonstrations was successfully completed February 28th, with a total of 16 flights and nearly 13 flight hours on the two vehicles.

The final Block 1 demonstrations verified safe operation of the weapons bay door at altitudes of 35,000 feet and speeds up to Mach 0.75, the maximum planned altitude and speed for the demonstrator vehicles. By the end of this year, we plan to use both X-45A demonstrators to work cooperatively in a simulated attack on a surface-to-air missile site, including dropping an inert munition.

To help arm tactical platforms, the High Energy Liquid Laser Area Defense System (HELLADS) program is developing a new high energy laser (HEL) tactical weapon system whose unique

cooling system might allow the system to be 10 times lighter, significantly smaller, and approximately half the cost of current developmental HEL systems.

The HELLADS design goal of less than 5 kilograms per kilowatt would enable, for the first time, high energy lasers that could be integrated into several air and ground tactical platforms, including unmanned combat armed rotorcraft (UCAR), UCAV, Predator B, the F/A-18, and future ground combat systems. HELLADS could protect fixed installations or population centers from attack, patrol a border, or patrol a demilitarized zone with the capability to react to hostile actions and engage tactical missiles, rockets, or artillery at the speed of light.



### Robust, Self-Forming Networks

The Department of Defense is in the middle of a transformation to what is often termed "network centric warfare." In simplest terms, the promise of network centric warfare is that military organizations and systems can be seamlessly networked to change the terms of any conflict to favor U.S. and coalition forces. It will allow the United States and our allies to go beyond a correlation of local forces by providing them better information and letting them plan and coordinate attacks far more quickly and effectively than our adversaries.

At the heart of this concept are survivable, assured, spectrum-agile communications, encompassing both the strategic and tactical levels. The goal of this work is a high capacity network that degrades softly under attack, while always providing a critical level of service.

DARPA is conducting research in areas including self-forming, *ad hoc* networks; high capacity, multiband, multimode communications systems; ultra-wideband communications; spectrum sharing; information assurance; and low probability of detection/intercept/exploitation communications.

The Adaptive Joint C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) Node Advanced Concept Technology Demonstration (ACTD) program is a prime example of DARPA's research in multiband, multimode communications. The program, just getting underway, will focus on a single system payload that can provide a gateway for connecting previously incompatible radios into a network, while conducting signals intelligence, electronic warfare, and information warfare. The ACTD is a joint DARPA, Army, Air Force, Office of the Secretary of Defense, and U.S. Joint Forces Command effort to assess the military utility of a multirole radio frequency system and to develop an optimal concept of operations with the users.

DARPA's Small Unit Operations Situational Awareness System (SUO SAS) has developed a self-forming, self-healing *ad hoc* communication system for dismounted warfighters operating in difficult and complex environments, such as urban and wooded terrains.

The SUO SAS network allows the warfighter to covertly and securely communicate with his fellow squad members and automatically reports all squad member position locations, enabling both mission planning and mission execution monitoring. In October 2002 at Fort Benning,

Georgia, DARPA and the Army conducted a highly successful demonstration of SUO SAS enabling the rescue of a "downed" aircrew trying to "escape capture" in a city—a situation modeled on the events in Mogadishu, Somalia, in 1993.

DARPA transitioned SUO SAS technology to the Army Communications and Electronics Command (CECOM), where it is being integrated into the Soldier, Biological and Chemical Command's Objective Force Warrior program. CECOM is also leveraging the SUO SAS radio and networking technologies to accelerate the networking of DARPA's NETFIRES program, unattended sensors, intelligent munitions, communications relay, and robotic systems into the Army's transformation into the Objective Force.

Borne out of the need for rapid and efficient utilization of the shrinking military bandwidth, the neXt Generation (XG) Communications program will make 10 to 20 times more radio frequency communication spectrum available to the U.S. military by dynamically sharing unused spectrum across frequency, time, and space. It turns out that, on average, only a small portion of the commercial spectrum is actively used at any given moment, even though most of the spectrum is licensed for assumed 100 percent use. The key technology question becomes whether an XG system can exploit underutilized spectrum without interfering with the original licensee.

#### Detect, Identify, Track, and Destroy Elusive Surface Targets

The Department of Defense has steadily improved its ability to conduct precision strike for many years. Timely, accurate, and precise delivery of bombs and missiles helped the United States overthrow a hostile regime in Afghanistan in short order with very few American or unintended casualties. However, our experience shows that major challenges remain in target detection, identification, and tracking. It is still difficult to strike targets that are hiding, moving, or that require a rapid reaction by U.S. forces in order to be destroyed.

Providing a focused response to these challenges, DARPA is assembling the necessary sensors, exploitation tools, command systems, and information technologies to rapidly find and destroy ground targets in any terrain, in any weather, moving or not, at any time, with minimum accidental damage or casualties. To do this, we are working to seamlessly meld sensor tasking with strike operations, leveraging the development of platforms that carry both capable sensors and effective weapons.

Of course, this way of operating implies blurring or even erasing barriers between the Intelligence and the Operations functions at all levels of command. This is a difficult technical challenge that requires a joint approach and has potentially large implications for U.S. military doctrine and organizations—truly a DARPA-hard problem.

A good example of DARPA's efforts is the Affordable Moving Surface Targeting Engagement (AMSTE) program. AMSTE is demonstrating how, by making only minor modifications to existing and planned systems, U.S. forces can, for the first time, integrate information from multiple radars to precisely and rapidly destroy individual and multiple moving surface targets.

AMSTE tracks the moving target from long range and uses this tracking information to continuously redirect a modified, low-cost global positioning system (GPS)-guided gravity bomb like the Joint Direct Attack Munition (JDAM) to attack the target. In September, an F-14 flying at 20,000 feet over the Naval Air Warfare Center Weapons Division in China Lake, California, delivered two AMSTE-configured JDAMs to two different targets within a convoy 6 miles away moving at 18 miles per hour.

That same day, an F/A-18 launched a single, AMSTE-configured Joint Stand-Off Weapon from 30,000 feet and scored a direct hit on a single M-60 tank, 35 miles away, that was moving at 15 miles per hour in traffic with a convoy progressing in the opposite direction.

These demonstrations—that AMSTE can precisely engage moving targets at stand-off ranges using modified low-cost inventory weapons—offer a powerful transformational capability to U.S. warfighters. The Air Force is examining several of the technologies inherent in the AMSTE concept.

The Air Force has placed requirements for AMSTE technology into its next-generation intelligence, surveillance and reconnaissance (ISR) and weapons assets by requiring moving target engagement capabilities resident on both the Global Hawk and the MC2A platforms. The requirement also exists in the Navy and the Air Force to have a weapon with data links for the purpose of attacking moving targets.

#### Characterization of Underground Structures

Many potential U.S. adversaries are well aware of the U.S. military's sophisticated ISR

capabilities and global reach, so they have been building deeply buried underground facilities to hide what they are doing and to harden themselves against attack. Such installations can be used for a variety of purposes, including hiding ballistic missiles, protecting leadership, command and control, and producing weapons of mass destruction.

DARPA's Counter-Underground Facility program is meeting the challenge posed by the proliferation of these facilities. We are developing and demonstrating seismic, acoustic, electro-optical, radio frequency, and chemical sensor technologies to characterize underground facilities. The program activities will enable the warfighter to answer the questions: "What is this facility for? How busy is it now? What are its internal structures and vulnerabilities? How might it be attacked? Did our attack destroy the facility?"

### Bio-Revolution

DARPA's strategic thrust in the life sciences, dubbed "Bio-Revolution," is a comprehensive effort to harness the insights and power of biology to make U.S. warfighters and their equipment safer, stronger, and more effective.

Over the last decade and more, the U.S. has made an enormous investment in the life sciences—so much so that we frequently hear that we are entering a "golden age" of biology. DARPA is mining these new discoveries for concepts and applications that could enhance U.S. national security in revolutionary ways.

There is a growing recognition of synergies among biology, information technology, and micro/nano technology. Advances in any one area often benefit the others, and DARPA has been active in information technology and microelectronics for many years. DARPA also is able to bring other disciplines together with biology in ways that enhance the multidisciplinary exploitation of biology.

DARPA's Bio-Revolution thrust has four broad elements:

- *Protecting Human Assets* refers to the Biological Warfare Defense work mentioned earlier.
- *Enhanced System Performance* work is developing new systems with the autonomy and adaptability of living things by developing biologically inspired materials, processes, and devices embodied in systems such as biorobotics.

- *Enhanced Human Performance* is aimed at preventing humans from becoming the weakest link in the U.S. military by exploiting the life sciences to make the individual warfighter stronger, more alert, more enduring, and better able to heal.
- *Tools* are the variety of techniques and insights on which the other three areas rest.

Let me give you some example of our work here.

To find new approaches to locomotion and highly adaptive camouflage, researchers in our Enhanced System Performance programs are studying how insects run over rough terrain, geckos climb walls, flies avoid capture and how an octopus hides. Why? Imagine if our soldiers and equipment could use some of these same techniques.

Our Continuous Assisted Performance (CAP) program is investigating ways to prevent fatigue and enable soldiers to stay awake, alert, and effective for up to 7 consecutive days without suffering any deleterious mental or physical effects and without using any of the current generation of stimulants.

In a recent series of studies, a new class of drugs, ampakines, has been identified that appears to be effective in eliminating the negative effects of sleep deprivation. Monkeys deprived of sleep for 30 hours showed complete recovery from cognitive, brain electrical signal, and brain metabolism defects when given the drug. We are aggressively pursuing development of these drugs as replacements for current stimulants.

Another exciting effort is in the area of blood platelets. Platelets are tiny constituents of the blood that promote clotting and wound healing; platelets are our body's own "internal bandage." Obviously, it would be very helpful to have platelets on hand in theaters of war to treat our wounded soldiers.

Unfortunately, platelets are very fragile and perishable; they last only about five days, even under ideal refrigerated storage conditions. Researchers have tried for years to extend the storage life of platelets, to no avail. So, to date, platelets have not been readily available to military field hospitals.

DARPA's Metabolic Engineering program has funded research that combines a freeze-drying process for platelets with a sugar called trehalose. Just this winter, we have demonstrated that



mouse platelets processed in this way can be stored for up to 18 months in their desiccated state and then successfully rehydrated for use. If this technology works for human platelets, and tests are beginning, it could eventually make blood platelets available on the battlefield to save the lives of our wounded soldiers.

### Cognitive Computing

Many elements of the information technology revolution that have vastly increased the effectiveness of the U.S. military and transformed American society—time-sharing, interactive computing, the ideas behind the personal computer, the Internet—were spurred on by the vision of a scientist at DARPA in the 1960s and 1970s, J. C. R. Licklider. Licklider envisioned people and computers working symbiotically. He imagined the potential of computers seamlessly adapting to people as partners that handle routine information processing tasks. Thus people would be free to focus on what they do best—think analytically and creatively—and, thereby, greatly extend the powers of their minds, i.e., what they can know, understand, and do.

Despite the enormous and continuing progress in information technology over the years, it is clear that we are still quite short of Licklider's vision. While current information systems are critical to U.S. national defense, they remain exceedingly complex, expensive to create and debug, hard to integrate with each other, insecure, and prone to failure. And, they still require the user to adapt to them, rather than the other way around. Computers have grown ever faster, but they remain fundamentally unintelligent and difficult to use. Something dramatically different is needed.

In response, DARPA's Information Processing Technology Office (IPTO) is returning to its roots to take on Licklider's vision again in a strategic thrust called "cognitive computing." Cognitive computers can be thought of as systems that know what they are doing.

Cognitive computing systems will have the ability to reason about their environment (including other systems), their goals, and their own capabilities. They will be able to learn both from experience and by being taught. They will be capable of natural interactions with users and will be able to explain their reasoning in natural terms. They will be robust in the face of surprises and avoid the brittleness and fragility of previous expert systems.

### **DARPA's Enduring Foundations**

While DARPA's strategic thrusts are strongly driven by national security threats and opportunities, a major portion of DARPA's research emphasizes areas largely independent of current strategic circumstances.

These "Enduring Foundations" are the investments in fundamentally new technologies, particularly at the component level, that historically have been the technological feedstocks enabling quantum leaps in U.S. military capabilities. DARPA is sponsoring research in materials, microsystems, information technology, and other technologies that may have far-reaching military consequences.

These technologies often form enabling chains. Advanced materials enable new generations of microelectronics that, in turn, enable new generations of information technology. And information technology is the enabling technology for network centric warfare, which I discussed earlier.

DARPA's support of these enduring foundations naturally flows into its eight strategic thrusts with a fair amount of productive overlap. For example, some of the work under the Bio-Revolution thrust could also be considered part of the materials work and the information technology work is being reshaped by the Cognitive Computing thrust.

With this in mind, more than 40 percent of DARPA's budget is devoted to high-risk, high-payoff component technologies, consistent with a goal established by the Under Secretary of Defense (Acquisition, Technology and Logistics).

### **Materials**

DARPA maintains a robust and evolving materials program. Our approach is to emphasize those new materials opportunities and discoveries that might change way the military operates. In the past, DARPA's work in materials led to such technology revolutions as new capabilities in high-temperature structural materials for aircraft and aircraft engines, and the building blocks for the world's microelectronics industry. Today, our materials work builds on this heritage and includes:

- *Structural Materials:* low-cost, ultra-lightweight structural materials and materials designed to accomplish multiple performance objectives in a single system

- *Functional Materials*: materials with a nonstructural function such as advanced materials for semiconductors, photonics, magnetics, and other electronic materials
- *Mesosopic Machines*: materials that can be used for air or water purification and harvesting water from the environment
- *Smart Materials and Structures*: materials that can sense and respond to their environment
- *Power Generation and Storage*: materials focused on novel ways to generate and store electric power; e.g., advanced fuel cells and materials to extract energy from the environment.

We have designed, built, and flown a micro-UAV with a truly multifunctional wing. The vehicle is capable of carrying visible and infrared cameras, chemical and biological hazard detectors, and communications packages. The 13-inch wingspan, 170-gram vehicle, named "Wasp," is the first of its kind in which the load-bearing wing structure is also the battery powering the motor and sensor package. In its maiden flight last August, WASP flew continuously at 30 mph for 1 hour, 47 minutes. In comparison, the baseline normal wing vehicle, powered by a conventional primary cell battery, has an endurance of just 30 minutes.

A final example is the Morphing Aircraft Structures program, which is developing technologies to create adaptive wings for air vehicles, enabling them to radically change their shape in flight. These technologies would allow an air vehicle to fundamentally and dynamically vary its flight envelope (much like a bird does) to perform multiple, radically different roles.

Thus, we are developing a lightweight, actively controlled system of sensors ("nerves"), actuators ("muscles"), and structures ("skin and bones") that mimic the ability of animals to adapt to widely changing environments and threats. The vision is to transform military air vehicles from large expensive systems of piloted aircraft to smaller systems of autonomous aircraft with multiple roles (such as locating and destroying targets) combined into a single aircraft, rather than requiring a large number of individual, single-role aircraft.

### Microsystems

Microelectronics, photonics, and microelectromechanical systems (MEMS) are three core technologies for the U.S. military, enabling it to see farther, with greater clarity, and better communicate information in a timely manner.

DARPA is building on these accomplishments by shrinking ever-more-complex systems into chip-scale packages—integrating the three core hardware technologies of the information age into systems on a chip. It is at the intersection of microelectronics, photonics, and MEMS that some of the greatest challenges and opportunities for DoD arise.

The model for this integration is the spectacular reduction in transistor circuit size under Moore's Law: electronics that once occupied entire racks now fit onto a single chip containing millions of transistors. As successful as this progress has been, the future lies in increasing the level of integration among a variety of technologies to create still-more-complex capabilities.

A good example is the Molecular Electronics program. Within 10 to 15 years, today's dominant computer switch technology, CMOS (complementary metal oxide semiconductor) transistors, will reach its lower size limits and no longer advance according to Moore's Law.

Anticipating this, the Molecular Electronics program is seeking to replace CMOS transistors with molecular switches that are 100 to 1,000 times smaller and have the potential to reach a trillion switches per square centimeter. This development will reduce the size, weight, and power of processors and increase their performance, allowing greater computing power to be packed into ever smaller volumes, increasing the "smarts" of military systems while reducing the soldiers' load.

There has been solid progress toward this goal: in FY 2004, DARPA expects to demonstrate the first 16-kilobit memory based on molecular switches.

### Information Technology

In the fall 2002, using technology developed under DARPA's Mobile Autonomous Robot Software (MARS) program, a robot was deployed roughly 30 meters into an abandoned Pennsylvania coal mine and generated a three-dimensional map of the mine's rugged interior in real-time as the robot moved through the tunnel.

The flooded mine had been flooded and was partially drained in the days before the experiments. The ground was still covered with toxic mud and oxygen levels were too low for humans to breathe. When integrated onto a hardened robotic platform, this MARS volumetric mapping technology could be applied for detailed, robotic exploration of caves, such as those that U.S. warfighters encountered in Afghanistan.

Our Augmented Cognition program will directly, but noninvasively, measure the mental effort ("cognitive load") of the human user using advanced, near-infrared optical sensors to measure brain activity. The computational system will know and support the actual state of the user, rather than just infer the user's state or intentions.

This information will allow us to manipulate or vary the load so information can be presented to the warfighter in ways that reduce information overload and will take advantage of spare mental processing power. This technology will greatly enhance performance under high-pressure circumstances and fundamentally change the nature of the human-machine interface.

We will also create interfaces that adapt to the warfighter rather than the other way around, moving a long ways toward the interactive adaptations originally envisioned by Licklider.

I hope my remarks today have given you a sense of our programs, as well as a sense of our vision and ambitions, of which I am equally proud. Thank you for this opportunity to appear before the subcommittee today. I would be happy to answer any questions you have.



RECORD VERSION

STATEMENT BY  
DR. A. MICHAEL ANDREWS II  
DEPUTY ASSISTANT SECRETARY OF THE ARMY FOR  
RESEARCH AND TECHNOLOGY AND  
CHIEF SCIENTIST  
BEFORE THE  
SUBCOMMITTEE ON TERRORISM,  
UNCONVENTIONAL THREATS AND CAPABILITIES  
COMMITTEE ON ARMED SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES  
ON SCIENCE AND TECHNOLOGY

MARCH 27, 2003

NOT FOR PUBLICATION  
UNTIL RELEASED  
BY THE COMMITTEE ON  
ARMED SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES

**DR. A. MICHAEL ANDREWS II  
DEPUTY ASSISTANT SECRETARY OF THE ARMY  
(RESEARCH AND TECHNOLOGY)  
ON ARMY SCIENCE AND TECHNOLOGY PROGRAM  
MARCH 27, 2003**

**INTRODUCTION**

Mr. Chairman and Members of the Subcommittee thank you for the opportunity to describe the Fiscal Year 2004 Army Science and Technology (S&T) Program and the significant role S&T has in achieving the Army's Transformation to our Objective Force Capabilities.

We want to thank the Members of this Committee for your important role in making today's Army the world's preeminent land combat force and your support of today's S&T investments that will sustain this preeminence for our future soldiers. Your continued advice and support are vital to our success.

**TRANSFORMATION**

The 2004 budget funds the fourth year of Army Transformation. The science and technology investments in this budget pursue technologies that can be matured and rapidly transitioned to system development and procurement to enable Objective Force capabilities as soon as possible. We also fund an agile basic research program focused on enduring Army needs as well as paradigm shifting opportunities to further transform the Army. The Objective Force Army will provide the Joint Force Commander with even more versatile, full spectrum capabilities than today's forces with decisive combat power while requiring much less logistics support.

## **FUTURE COMBAT SYSTEMS (FCS)**

The Future Combat Systems (FCS) program transitions Increment I to System Development and Demonstration in Fiscal Year 2003. However, at \$625M FCS remains the single largest S&T investment in the Fiscal Year 2004 budget. This investment will provide advanced technology for FCS capabilities beyond Increment I using a spiral development acquisition approach to insert advanced technology as it becomes available.

The FCS represents a true paradigm shift in how we fight. In the Army's quest for true innovation, it established a partnership with the Defense Advanced Research Projects Agency (DARPA) in 2000 to explore innovative FCS concepts and technologies. This partnership has been successful in pursuing several innovative technology solutions from the Army S&T program, DARPA's core investments, industry partners, as well as international sources that are now being "harvested" by the FCS Lead Systems Integrator—Boeing/Systems Applications International Corporation team. The FCS is not "a platform," it is a family of 18 systems plus the soldier and the network. It is a system of systems—battlefield capabilities in which the whole exceeds the sum of its parts.

The FCS system of systems is based on information age technologies, embedded in manned and unmanned air/ground platforms, as well as integrating long-range air- and ground-based sensors with long-range cannon and missile precision munitions, to enable "Network-Centric Warfare." Key technologies include: Fully networked secure, non line-of-sight, On-the-Move Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR); beyond line-of-sight cannons; stand-off precision and loiter attack missiles; advanced signature management; active protection; advanced armor; and hybrid electric propulsion. In addition, FCS will incorporate embedded, real-time interactive, simulations for training and mission rehearsal. The Army is on track to achieve the FCS first unit equipped (FUE)—one battalion equivalent—in 2008 and an initial operating capability of one brigade Unit of

Action (UoA) in 2010.

### **OBJECTIVE FORCE WARRIOR**

Another major S&T investment is Objective Force Warrior (OFW) that will enable follow-on increments of FCS. The OFW will provide capabilities to the individual soldier that is achievable only at the platform-level today. Through networked connectivity to the FCS-equipped maneuver Unit of Action (UoA), OFW will enable revolutionary lethality, mobility, survivability, and sustainability for the individual soldier while reducing logistics demands. By the end of 2006, the OFW program will demonstrate increased individual soldier lethality and survivability through netted communications and fires while reducing the soldier's physical load from over 90 lbs to a goal of 40 lbs. The program develops a lightweight, low-observable, enhanced-armor protection fighting ensemble. Other key technologies include lightweight, high-efficiency power sources; embedded physiological monitoring and limited medical treatments; multi-functional light-weight materials; embedded training; and networked sensors to enable unparalleled situational understanding.

### **COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) INITIATIVES**

The S&T investments in C4ISR initiatives will enable network-centric Objective Force operations. These efforts allow sensor and processing technology to see, understand and shape the battlespace before the enemy can react—increasing combat force effectiveness and survivability. The S&T program will develop and demonstrate real-time, continuous situational understanding by integrating data from manned and unmanned air- and ground-based sensors. Technologies include: Next generation, high performance multispectral sensors (electro-optic, infrared, radio frequency, acoustic, seismic,

chemical); algorithms and intelligent agents to integrate data from a wide variety of networked sensors (airborne and ground); adaptive, self-healing Command & Control and Communications (C3) networks; and high-data rate processors. We have made significant progress in the past 18 months in realizing network-centric capabilities through our C3 On-The-Move Advanced Technology Demonstration program at Fort Dix, New Jersey. This S&T demonstration is providing new insights for commander-centric operations for our warfighters while transitioning prototype-like products to current capabilities.

## **UNMANNED SYSTEMS**

Unmanned Systems will be integral in future UoA operational concepts. These will expand the envelope of warfighting capabilities while reducing risk to soldiers and the logistics footprint of the force. The S&T program is pursuing a wide spectrum of technologies for unmanned air and ground systems. The goal is to enable an overmatching ground combat force where up to 33 percent of its systems are unmanned by 2015. Unmanned systems will range in size from manportable to large cargo-lifting unmanned air vehicles (UAVs) or unmanned ground vehicles (UGVs).

Small UGVs can be employed in complex terrain (MOUT and jungles) to provide continuous information superiority. Larger UGVs can perform high-risk (minefield breaching, attack well-armed threats, chemical bio detection) or routine functions (truck re-supply, soldier mule, and medical evacuation). Realizing the full potential of unmanned systems requires technology development in areas including sensors for navigation and mission performance, intelligent systems for semi-autonomous or autonomous operation, networked communications for manned-unmanned teaming, and human-robotic interfaces.

Army S&T is investing in UAVs for the soldier and for the FCS family of systems. Our smallest UAV is the Micro Air Vehicle (MAV), a 9-inch, 8-ounce ducted fan UAV that can be carried and launched by an individual soldier. It is



being matured as an Advanced Concept Technology Development (ACTD) and will be ready by 2005. The Army is also maturing the Organic Air Vehicle (OAV), a larger scale – 19-inch – ducted fan UAV designed to be launched from an FCS platform. The OAV is in competition for FCS Increment I. Small UAVs provide new capabilities for reconnaissance, precision targeting, extended range communications, and stand off-precision fires in support of the warfighter. The major S&T UAV investments are in larger UAVs. The A-160 Hummingbird will meet medium altitude long endurance requirements to provide communications relay and intelligence, surveillance, and reconnaissance for the UoA. The A-160 Hummingbird is undergoing flight testing now in California with transition scheduled for Fiscal Year 2007.

In 2002, the Army established a new agreement with the Defense Advanced Research Projects Agency (DARPA) to develop the Unmanned Combat Armed Rotorcraft (UCAR). By 2006 this program will demonstrate the first flight prototypes fully autonomous, armed, low-observable, unmanned rotorcraft capability for deep tactical strike and Reconnaissance, Surveillance and Target Acquisition (RSTA) missions. The UCAR program exploits the agility, flexibility, and responsiveness inherent in armed rotorcraft systems to provide a highly survivable, lethal option to the Objective Force, taking the soldier out of harm's way. Rotorcraft provide the unique ability to perform stationary hover to acquire and engage targets in complex terrain and Military Operations on Urban Terrain (MOUT) environments, as well as enable enhanced survivability through the ability to perform rapid acceleration and evasive maneuvers. The UCAR program matures next generation autonomy, collaborative operations, and command and control technologies. The UCAR can be an independent weapon/RSTA system in FCS, or teamed with manned systems like RAH-66 Comanche.

## **TECHNOLOGY TRANSITION**

Successful transition of Army S&T is central to enabling the Army Vision. The Army S&T community has been challenged to develop a revolutionary warfighting capability within an accelerated timeframe. To accelerate technology transition, the Army adopted aggressive management practices and methodologies to manage risk. The Army adopted Technology Readiness Levels (TRLs) as the method to measure the maturity of the technologies being developed. TRLs were identified in the recommendations put forward in the 1999 General Accounting Office (GAO) Report<sup>1</sup> citing best practices for the management of technology development. The GAO stated that critical technologies and/or subsystems should be at a high level of maturity prior to making the commitment for development and production of a weapons system. The Army has adopted this approach and is using TRLs to track and communicate technology maturity levels to the acquisition community. We can take time out of the transition process by maturing technology in the S&T phase to greater than TRL 6 – system/subsystem prototype demonstration in a relevant environment. By doing this, we spend more in S&T, but save time and money in Systems Development and Demonstration (SDD), then proceed faster to production.

Risk management is another tool designed to improve the transition of advanced technologies to the warfighter by providing the gaining acquisition Program Manager with a risk assessment and risk mitigation plan for S&T programs. While Technology Readiness Levels assess the estimated maturity of a technology, the risk management process focuses on identifying, tracking, and managing potential cost, schedule, and performance risks.

### **COUNTERMINE TASK FORCE**

Mine detection, neutralization, and minefield breaching have been enduring Army challenges that must be overcome to enable Objective Force Full-

---

<sup>1</sup> "BEST PRACTICES: Better Management of Technology Development Can Improve Weapon Systems Outcomes," GAO/NSIAD-99-162, July 1999

Spectrum operations. The Army has established a Science and Technology Countermine Task Force (STCTF) to develop integrated, holistic Countermine S&T program proposal(s) to accelerate transition of innovative technologies to satisfy the Army's Countermine mission needs. The Task Force will:

- Suggest technology investment areas and priorities and identify technical and integration risks affecting the accelerated transition of technology to enable Objective Force Countermine Operations;
- Examine expansion of countermining capabilities that leverage future sensors, processors, and management of large numbers of sensors with assured connectivity;
- Examine solutions for rapid mine neutralization and minefield breaching considering the full-range of potential manned and unmanned platform applications, air and ground based;
- Consider the full-range of science and technology opportunities from basic research through advanced technology development and provide recommendations for near and far term options; and
- Identify countermeasures that may affect countermining technology solutions.

## **LOGISTICS S&T**

The revolutionary capabilities projected for the Objective Force will not be achieved until there is a corresponding revolution in military logistics. Reducing the logistics "drivers" -fuel, ammunition, maintenance, and water - will enable speed and agility in the Force. Some of the key enabling technologies for logistics reduction include: On-board water generation; real-time logistics command and control (Log C<sup>2</sup>) and distribution management; enhanced multi-purpose munitions and packaging; fuel efficient propulsion and power technologies; real-time diagnostics and prognostics; and microelectromechanical systems (MEMS).

## **BASIC RESEARCH PROGRAM**

The Army Basic Research program produces new understanding to enable revolutionary advances and paradigm shifts in technology to enable the Army's Transformation goals. This program invests in world-class expertise (government, academia and industry) and state of the art equipment to explore fundamental phenomena and exploit scientific discovery. These investments are key to the Army's ability to win the race for speed and precision. Today, Global Positioning Systems, night vision devices, and precision-guided munitions are essential to all our operations. These capabilities can be traced to sustained basic research investments in decades past. The Army's Basic Research program has three components: World class university-based research to support single investigators and focused centers to enable paradigm shifting capabilities such as nanotechnology for the soldier; research at centers that advance enduring needs in the areas of rotorcraft and automated technologies; and industry led centers focused on robotics, power and energy, communication networks, display technologies, and decision aids. It exploits advances in emerging, high payoff technologies such as nanotechnology, biotechnology, robotics, immersive environments, directed energy, and very high performance computing

## **CONCLUSION**

The Army must have a diverse S&T portfolio that is responsive to current and future warfighter needs. The S&T community seeks technological solutions that can be demonstrated in the near-term, explores the feasibility of new concepts for the midterm, and explores the imaginable for an uncertain far-term future. Since the Army vision was announced in October 1999, the Army S&T

effort has been reshaped, refocused, and reinforced to speed the development of those critical technologies essential to transform the Army into the objective force. The Army S&T community has accepted the technical challenges embraced in the Army Vision. We have committed our intellectual resources—our people—and our facilities and funding to maintain the momentum of the Army's Transformation!



NOT FOR PUBLICATION  
UNTIL RELEASED BY THE  
HOUSE ARMED  
SERVICES COMMITTEE

STATEMENT OF

RADM JAY M. COHEN  
CHIEF OF NAVAL RESEARCH

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

ON

DEFENSE SCIENCE AND TECHNOLOGY POLICY AND PROGRAMS  
FOR FISCAL YEAR 2004

27 MARCH 2003

NOT FOR PUBLICATION  
UNTIL RELEASED BY  
THE HOUSE ARMED  
SERVICES COMMITTEE

Mr. Chairman, distinguished members of the subcommittee, thank you for this opportunity to discuss Naval Science and Technology. You and the other members of the Senate Armed Services Subcommittee on Emerging Threats and Capabilities have been leaders in calling attention, both nationally and in the Department of Defense, to the importance of moving new technology quickly from the scientist's bench to our Sailors and Marines.

Let me begin, with an overview of our scientific and technological portfolio. The return on the Nation's investment in Naval science and technology is measured in capabilities. This is particularly important in a time when we must not only fight and win a global war, but also transform the Navy and Marine Corps. We hear a great deal about al Qaeda and others posing an "asymmetric threat" to us. But our scientific and technological edge gives us a tremendous asymmetric advantage over our enemies. We've already seen some of that advantage at work in Operation Enduring Freedom, and Naval transformation will depend on our ability to sustain and exploit our lead in science and technology. To do that you need a long-term, stable, and sustained investment in science and technology transitioning to research and development, validated through on-going experimentation, with transition to the Fleet and Force in a continuous cycle of progress.

It is difficult to exaggerate the importance of sustained scientific effort: investment in research is always a long proposition. We have seen some very quick delivery of new, advanced capabilities already in this war. These can seem like overnight successes. Take the thermobaric bombs our forces dropped on al Qaeda and Taliban positions last year in Gardez, Afghanistan. That thermobaric fill—developed at Naval Surface Warfare Center Indian Head, and weaponized by the Navy in collaboration with the Defense Threat Reduction Agency and the Air Force—was more than 30 years in preparation. This particular Naval investment in basic, synthetic organic chemistry (for that's what produced thermobarics) began in the late 1960s after the disastrous accident and fire aboard USS FORRESTAL. So basic science answered a Naval need, and the necessary work had been done to produce an effective, new class of weapons. You might consider it an overnight success that depended on 30 years of work.

With this in mind, I am pleased to report that the Department of the Navy's science and technology funding has shown real growth from FY 2003 to FY 2004 (based on comparison of the President's Budget Requests for those years). This is our positive response to the Defense guidance and Congressional mandates that have called for more Defense science and technology funding. During FY2004 budget development, the Department of the Navy's Science and Technology Future Years Defense Plan (FY 2004-FY 2009) was increased by a net \$1.45B.

The significant increases in FY 2004 include programs that are both transformational and bear directly on the current war:

- Naval Unmanned Combat Air Vehicle +\$98M
- National Aerospace Initiative-Supersonic Cruise Missile +\$22M
- Strategic Systems Infrastructure +\$20M
- Joint Project Office - Special Technology Countermeasures +\$14M
- US Coast Guard Vessel Tracking +\$10M

The Department of the Navy is gratified by consistent Congressional support of our science and technology program. We trust that we are managing that support effectively to achieve the objectives of our program.

We are particularly gratified by Congressional interest in testing and evaluation—we owe Sailors and Marines the assurance that the systems we put in their hands work as advertised, especially when they're delivered under wartime exigencies. Regarding, for example, the Defense Test Resource Management Center Congress has recently mandated, the Department of the Navy certainly supports the concept. We are working with the Under Secretary of Defense for Acquisition, Technology, and Logistics to support the establishment of this new field activity, and we look forward to supporting its mission.

Let me return to my earlier theme of transformation in a time of war. To keep perspective, recall that transformation occurs over the near-term, mid-term, and long-term. Naval science and technology is a sustained journey from discovery to deployment in which innovation (invention) and experimentation (validation) transform the operating forces. Because

this is a continuous cycle, we find technological advance in “Today’s Navy and Marine Corps,” the “Next Navy and Marine Corps” (roughly the forces that will emerge over the next five to fifteen years), and the “Navy and Marine Corps After Next”—which we will see in fifteen to thirty years.

How do we choose where we invest? We are guided by:

- ***Programs for Rapid Response***—immediate feedback from the operating forces. We get this through participation in experimentation with those forces, in exercises like Millennium Challenge, through the Naval Research Science Advisors posted to the staffs of each major Navy and Marine Corps Command, and through our Tech Solutions initiative. When an immediate challenge, problem, or opportunity lends itself to scientific resolution, we are able to shift a relatively small but nonetheless crucial investment to a decisive area.
- ***National Naval Responsibilities***—fields in which the Department of the Navy is the only significant U.S. sponsor. These include fields like Naval Engineering, Ocean Acoustics, and Underwater Weaponry. If the Department of the Navy didn’t invest in them, it’s unlikely that anyone would. It’s vital to keep such fields healthy, not only for the sake of our own capabilities, but to avoid technological surprise as well.
- ***Naval Science and Technology Grand Challenges***—big, difficult, challenges that, if met, could give us decisive capabilities fifteen to thirty years in the future. We encourage the nation’s scientific community to achieve breakthroughs in difficult but achievable scientific challenges like Naval Battlespace Awareness, Advanced Electrical Power Sources for the Navy and Marine Corps, Naval Materials by Design, and Multifunctional Electronics for Intelligent Naval Sensors.
- ***Future Naval Capabilities (FNCs)***—programs to shape the next Navy and Marine Corps. Developed and managed by integrated product teams with members of the acquisition, requirements, science and technology, resource, and above all warfighter communities, the Future Naval Capabilities fill the gap that all too often opens between science and technology on the one hand and acquisition on the other.

A great deal of our transformational effort is lodged in the Future Naval Capabilities. Science and technology enable Navy transformation by achieving the FNCs' goals. The key to successful transformation is the strong business partnership among scientists, industry, requirements, acquisition, and warfighters.

The FNC process delivers maturing technology to acquisition program managers for timely incorporation into platforms, weapons, sensors, and process improvements. With a total investment of \$577.6 million in FY02 and over \$640 million in FY03 and \$500 million planned for FY04, FNCs support the Secretary of the Navy's goals to 1) increase combat capability, 2) enhance personnel performance, 3) introduce advanced technology, and 4) improve business practices.

The Office of Naval Research devotes approximately two-thirds of its 6.3 (advanced technology development) funds and about two-fifths of its 6.2 (applied research) funds to Future Naval Capabilities. As you know, we currently have twelve approved Future Naval Capabilities. I'll describe each one briefly, and provide the basics as to where it fits into the Department of the Navy's concept of Sea Power 21:

- **Autonomous Operations** – This program is pursuing a dramatic increase in the performance and affordability of Naval air, surface, ground, and underwater autonomous vehicles—unmanned systems able to operate with a minimum of human intervention and oversight. The Autonomous Operations Future Naval Capability gives us a great potential to operate effectively in what would otherwise be denied areas. It contributes to *Sea Shield* and *Sea Strike*. In FY 2004, for example, we will transition the Gladiator Tactical Unmanned Ground Vehicle to the Marine Corps. Gladiator is intended to support dismounted infantry across the spectrum of conflict and throughout the range of military operations. It will enhance tactical commanders' ability to detect, identify, locate, or neutralize a broad range of threats.
- **Capable Manpower** – The focus here on affordable human-centered systems that give our Sailors and Marines the ability to operate effectively under conditions an enemy can barely survive. The primary goal of this program is to get the right person in the right job with the right training at the right time in order to meet the needs of the Navy and Marine



Corps. A great deal of progress has been made in this last area. In particular, two products have already transitioned: Models of Navy Compensation and Personnel Behavior (MODCOMP)—a tool for manpower analysts to rapidly develop retention forecasting models through ready-access to relevant data sources, intuitive linkage to highly sophisticated statistical tools, and export capability to populate existing decision support tools, and Comprehensive Officer Force Management Environment (CHROME)—a tool for monitoring actual officer inventory behavior and a 12-month loss-forecasting model to predict officer losses for each primary category. Capable Manpower is most directly aligned with *Sea Warrior*.

- **Electric Warships and Combat Vehicles** – The future of Naval warfare is electric. Warships will have revolutionary power plants that permit new hullforms and propulsors, reduce manning, streamline logistics, power advanced sensors, and enable future high energy and speed-of-light weapons. We have already successfully demonstrated the essential elements of a high temperature superconducting motor for the next generation of warship, and a hybrid diesel-electric reconnaissance vehicle for the Marines. This Future Naval Capability is aligned most closely with *Sea Strike*, *Sea Shield*, and *Sea Basing*.
- **Fleet/Force Protection** – We have very capable ships, aircraft, and ground combat vehicles. It's our business to ensure that they don't fall to the sorts of asymmetric threats our enemies pose. This Future Naval Capability, aligned with *Sea Shield*, is working to develop effective organic means of protection: weapons, sensors, countermeasures, stealth and damage control. It has already transitioned Real Time Damage Detection, Assessment, and Response to acquisition. As well, the President's Budget for Fiscal Year 2004 supports the execution of full-scale development of an Integrated Torpedo Defense System for protection of heavy combatants and amphibious forces operating in the challenging littoral environment. This effort is the culmination of support, from the Congress, for torpedo defense R&D activity over the past several years, and is focused on the ability to rapidly deliver threat-sensitive capabilities to the Navy's high value forward deployed assets.
- **Knowledge Superiority and Assurance** – Information technology is as crucial to Naval superiority as it is to any other aspect of contemporary life. This program is developing our ability to distribute integrated information in a dynamic network with high

connectivity and interoperability. It will ensure knowledge superiority, common situational understanding, and increased speed of command. Knowledge Web technology from this program has been deployed with the USS Carl Vinson Battle Group, now engaging the enemy in Operation Enduring Freedom. This Future Naval Capability is a key enabler of *FORCEnet*.

- **Littoral Antisubmarine Warfare** – This program is part of our shift of emphasis to littoral, expeditionary operations. The antisubmarine warfare challenge in coastal waters is a tough one, so we focus scientific effort on enhancing our ability to detect, track, classify, and engage enemy submarines in a near-the-shore environment before they are close enough to harm our forces. A number of products have already entered acquisition from this program: the Environmentally Adaptive A/N SQQ-89 sonar instrumented tow cable fibers and signal processing, for example. *Sea Shield* will benefit from the products of this Future Naval Capability.
- **Littoral Combat and Power Projection** - This Future Naval Capability has two major thrusts: Expeditionary Logistics (an important step toward *Sea-Basing*) and Littoral Combat (essential to *Sea Strike*). It focuses on deploying uniquely capable combat and logistics systems necessary to deploy and sustain the Fleet and the Force without building up a large logistical infrastructure ashore. The program has already transitioned a baseline logistics command and control system for expeditionary warfare.
- **Missile Defense** – This program is directed at the threat expeditionary forces face from cruise missiles. In particular, it's working toward the ability to track and destroy overland cruise missiles that threaten both ships at sea and Marines ashore. It will also contribute to our general air defense capability through a single integrated air picture, composite combat identification, distributed weapons control, and overland intercept capability. This new capability will greatly mitigate the likeliest and most dangerous air threat to our forces. The Missile Defense Future Naval Capability is nearing transition in several of its product lines, including, for example, the Reactive Materials Warhead and Affordable Ground-Based Radar. Missile Defense forms an important part of *Sea Shield*, but this shield is extended to cover forces ashore, as well.
- **Organic Mine Countermeasures** – Mines are a cheap, deniable, and able to infest the battlespace with a menace far out of proportion to their numbers, mines have been and

will continue to be deployed against us by terrorists and their state sponsors. We're working to give our forces an organic—that is to say, an inherent—ability to detect, characterize, and neutralize mines wherever they may be encountered. Closely aligned with *Sea Shield*, this Future Naval Capability has transitioned several important products. One of them, the REMUS autonomous underwater vehicle, is now in the hands of our operating forces. It was pressed into service in the weeks immediately following 9/11 to help secure ports on both of our coasts. REMUS emerged from a basic oceanographic research program—another piece of evidence that overnight successes are long in preparation.

- **Time Critical Strike** – Here we are substantially reducing the amount of time it takes to hit critical mobile targets, like theater ballistic missiles, command centers, and weapons of mass destruction. One of this Future Naval Capability's products, the Affordable Weapon (a loitering cruise-missile-like system that can carry a variety of payloads) is being deployed to the CENTCOM area of responsibility soon. Time Critical Strike is aligned with *Sea Strike*.
- **Total Ownership Cost Reduction** – This Future Naval Capability is using advanced design and manufacturing processes to decrease significantly the cost of buying, operating, and maintaining our systems. We are working to reduce total lifecycle costs, and that includes obvious work in design and manufacturing as well as less obvious savings realized from reduced manning, better environmental compliance, and more sophisticated cost-estimating tools. Aligned most especially with *Sea Enterprise*, this Future Naval Capability has transitioned a number of products to industry. One example includes advanced coating techniques for hot-running turbine engines.
- **Warfighter Protection** – Improved casualty prevention, care, and management are the goals of this Future Naval Capability. Aligned with *Sea Shield* and *Sea Warrior*, this program has already transitioned a life-saving clot-inducing bandage to our forces in Afghanistan.

Our investment portfolios are not built in isolation. The Defense Reliance process integrates the Services' science and technology programs while preserving the healthy diversity of vision and approach that has given us the technical agility we enjoy today. And our relations

with the Defense Advanced Research Projects Agency (DARPA) are excellent and productive. Much of the Office of Naval Research's basic and applied research investment is designed with a view to handing scientific advances over to DARPA for further development and exploitation. The Unmanned Combat Air Vehicle – Naval (UCAV-N) program is an excellent example of this kind of collaboration.

I will now address some of our challenges concerning the health of the Navy's Laboratories and Warfare Centers. The Naval Research & Development Centers, which include the SYSCOM Warfare Centers, the Naval Research Laboratory (NRL) and the Medical and Health Research Centers, employ world-class technical experts who execute much of the Navy's science and technology portfolio, developing innovative solutions and transformational capabilities for the Navy and Marine Corps. These centers, spread throughout the United States, currently employ around 40,000 civilians, about half of who are scientists and engineers. They perform cutting edge work upon which we depend to preserve its military superiority. The effectiveness of the war-fighting systems employed by the Navy and Marine Corps of the Future depends as much on investment in these dedicated, capable civil servants as it does on the size of the science and technology budget itself.

The past decade's frequent downsizings, coupled with the declining number of American students—particularly women and minorities, pursuing mathematics, engineering and physical science degrees—has left us with a dwindling pool of scientists and engineers available to become the next generation of researchers. This situation jeopardizes our ability to perform essential research in support of, ultimately, Sailors and Marines.

Recent warnings about the decline of the Navy's S&T workforce come from a variety of sources. In the Naval Institute's *Proceedings*, Dr. James E. Colvard, former director of civilian personnel policy for the Department of the Navy and chair of the panel that developed the report, "Civilian Workforce 2020, Strategies for Modernizing Human Resources Management in the DON" notes the Navy has "put its institutional capability in science and engineering at peril." Colvard also comments, "The Navy has lowered its level of intellectual involvement in research

and development and weakened its entire infrastructure, which at the end of WWII was the strongest in the world.”

The DoN’s “Civilian Workforce 2020” study pinpointed workforce modernization as the defining issue pushing S&T revitalization. The study concluded: “It is not possible to achieve a functional workforce that is prepared to meet the management, technical, and political challenges of the future without investing financial resources and leadership attention.”

Recently, a tri-Service laboratory study chartered by the Director, Defense Research and Engineering, and carried out under the auspices of the Naval Research Advisory Committee produced a report: *Science and Technology Community in Crisis*. In the report, the panel commented that all of the laboratories they visited reported that “maintaining a quality scientific and engineering staff is growing more difficult.” The report continued: “The real issue is not whether the laboratories can muddle through under the current system and fill Science & Engineering vacancies with entry-level personnel. It is whether they can compete effectively for, and retain, the best and brightest technical talent, e.g. the top 10 percent.”

A total commitment to improving our ability to attract and retain a cadre of world-class scientists and engineers will be necessary to meet the simultaneous challenges of performing transformational research while replenishing the aging talent base. Simple demographics show that over the next 10 years we will lose most of our current workforce. Although some organizations are holding their own in recruitment, many indicators are going negative, and managers report greater difficulty in hiring quality scientific personnel. If we cannot invest at an appropriate level in promising research scientists and engineers today, we believe that the options and opportunities the Naval R&D labs and center have provided our fighting forces for more than the past 60 years or more will begin a decline that will be difficult to reverse.

The Navy has launched an initiative called “N-STAR”—Naval Science and Technology for Advancing Revitalization. This program is addressing the personnel issues associated with: refreshing our technical workforce with the small pool of recruits available to fill positions vacated by retiring scientist and engineers, and with the professional and technical enhancement of the current workforce as they move into senior positions at the Naval Research and



Development Centers. N-STAR is a collaborative effort, concentrating on integrated relationships with partners within the university community and other federal agencies interested in the future of the nation's scientific and engineering workforce.

In Fiscal Year 1995, Congress provided the Department of Defense labs with the opportunity to test a variety of new personnel tools. Section 342 of the Fiscal Year 1995 National Defense Authorization Act permitted some of our labs and centers to implement a number of personnel reforms not previously available. The personnel initiatives being tested under this program have broad acceptance and are achieving very positive results.

For several years now, the Department of Defense has been actively testing many management flexibilities, i.e. pay banding, pay for performance and simplified classification. Acknowledging the success of the demonstration projects and alternate personnel systems, the Under Secretary of Defense for Personnel & Readiness began a review of the personnel management flexibilities already in use within the Federal Government. Multi-Component, multi-functional work teams and senior functional executives completed this yearlong review that identified "best practices" - those with the highest rate of success. The Office of the Secretary of Defense is considering many of these best practices for inclusion in a legislative proposal on human resource management.

In conclusion, the return on the nation's investment is clear. Naval transformation depends on a long-term, stable, and sustained investment in science and technology, validated through on-going experimentation and transition to the warfighter in a continuing cycle.

Mr. Chairman, thank you again for the opportunity to share with the Subcommittee some of the good things the Navy is doing in the S&T world.

DEPARTMENT OF THE AIR FORCE

PRESENTATION TO THE HOUSE ARMED SERVICES COMMITTEE  
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS, AND  
CAPABILITIES

UNITED STATES HOUSE OF REPRESENTATIVES

SUBJECT: Fiscal Year 2004 Air Force Science and Technology

STATEMENT OF: Mr. James B. Engle  
Deputy Assistant Secretary  
(Science, Technology and Engineering)

March 2003

NOT FOR PUBLICATION UNTIL RELEASED  
BY THE ARMED SERVICES COMMITTEE,  
UNITED STATES HOUSE OF REPRESENTATIVES

## **INTRODUCTION**

Mr. Chairman, Members of the Subcommittee, and Staff, I very much appreciate the opportunity to provide written testimony on the Fiscal Year 2004 Air Force Science and Technology (S&T) Program. The United States Air Force is transforming to a capabilities-focused Expeditionary Air and Space Force. We are doing this through the development of the Concept of Operations for each of the seven major tasks the Air Force must be capable of accomplishing. Our goal is to make the warfighting effects and the capabilities we need to achieve them the drivers for everything we do. This is especially true in our S&T Program. We have taken the effects and capabilities required by the seven Concepts of Operations and mapped them to the Long-Term Challenges and Short-Term Objectives identified in the Congressionally-directed S&T Planning Review completed in February 2002. Not surprisingly, we have a high correlation between our S&T programs and the capabilities required by these Concepts of Operations. This is because the Air Force Research Laboratory (AFRL) closely links the technologies reflected in its S&T Plan to warfighter capability needs.

The United States Air Force is committed to a robust S&T Program that enables us to achieve our vision of becoming an integrated air and space force capable of rapid and decisive global engagement. By continuing our investment in transformational technologies that support a reduced cycle-time, spiral development acquisition process, the Air Force will retain its dominance of air and space in future conflicts, against both traditional and asymmetrical threats.

Innovation is a vital part of our heritage and is key to ensuring the Air Force will meet the challenges of tomorrow. Transforming our warfighting capabilities towards this end will involve continued innovations in how we think about employing our forces to defend our nation, as well as quantum leaps in our technology. We must be prepared to counter regional instabilities, the

worldwide availability of advanced weapons, and other emerging and less predictable asymmetrical threats. We are developing transformational technologies that permit flexible forces to operate far from home, on short notice, and for extended time periods. However, we must also be able to afford these innovations once we develop them in order to re-capitalize the Air Force to fulfill our vision. To meet these objectives, we search out the most promising and affordable technologies in order to win decisively, protect our forces, and minimize collateral damage.

#### ***S&T BUDGET/SENIOR LEADERSHIP INVOLVEMENT***

We have been faced with the reality of a fiscally-constrained, but operationally-demanding environment. The high operations tempo the Air Force has sustained in support of peacekeeping operations and conflicts, such as Afghanistan, has placed a great burden on our people and system.

In spite of these requirements, the Air Force is working to increase S&T funding, while maintaining a balanced S&T portfolio. The Air Force Fiscal Year 2004 President's Budget (PB) request for S&T is \$2.2 billion, an increase of more than \$535 million from the Fiscal Year 2003 PB. A significant addition to S&T in Fiscal Year 2004 is over \$160 million for the Office of the Secretary of Defense's Director of Defense Research and Engineering's (DDR&E's) National Aerospace Initiative. However, the most significant change in the S&T PB request results from the devolvement of \$350 million for several Office of the Secretary of Defense efforts to the Air Force S&T Program. This includes the High Performance Computing Modernization program, the University Research Initiative program, and the High Energy Laser Joint Technology program.

The Air Force understands the concerns of Congress regarding the level of support for these devolved programs and is working hard to ensure execution of the programs transferred to the Air Force continues to support the diverse multiple military objectives inherent in each of these programs. Further, the Office of the Secretary of Defense will continue to provide policy guidance and oversight for these efforts.

In a separate action, the Seismic Research Program for detection of nuclear explosions has been transferred back to the Air Force from the Defense Threat Reduction Agency (DTRA). The Air Force is working to reinvigorate the seismic research expertise we possessed before transfer of the program to DTRA in 1997.

One area in which the Air Force has increased its investment is in space communications technology with initiation of the transformational communications technology development program. This program will identify, develop, and demonstrate the wideband technologies needed to build a space-based laser communications network that could provide higher data throughput to transform our military satellite communications infrastructure.

In conjunction with the increase in S&T funding, there has also been a significant increase in the involvement of the warfighting commands and senior Air Force leadership in the planning, programming, and prioritizing of Air Force S&T. For example, the Secretary of the Air Force, the Air Force Chief of Staff, and the Air Force four-stars and other senior leaders review the S&T portfolio. The latest senior leadership review focused on transformational technologies that can be developed to assist in combating terrorism and other asymmetrical threats.



## **WORKFORCE**

The Air Force scientist and engineer (S&E) workforce is another area where senior Air Force leadership involvement plays a pivotal role. Both Secretary Roche and Gen Jumper are deeply involved in shaping our future S&E workforce. Air Force civilian and military S&Es are highly motivated and productive. The Air Force is unique in that 20 percent of its laboratory S&E government workforce is active duty military. This gives us a direct link to the warfighter. Some of these military S&Es come directly from operational commands, while others will serve in operational commands later in their careers.

The Air Force is committed to shaping its S&E workforce with the vision to enhance excellence and relevance of S&T into the 21<sup>st</sup> Century and appreciates the support Congress has already provided. This challenge requires the Air Force to maintain a dominant edge in technology and also requires us to provide clear direction and growth for our S&E workforce. However, we, as do others, find it is difficult to recruit and retain S&Es. The Air Force has several initiatives, both civilian and military, that address recruitment and retention issues.

AFRL was the first laboratory in the Department of Defense (DoD) to take advantage of legislation allowing us to experiment with alternative personnel management systems for our civilian S&Es. The simplified classification system, broadband pay levels, and contribution-based compensation that form the cornerstone of the Air Force Laboratory Demonstration Project have provided AFRL with some key flexibilities needed to compete with private industry for critical S&E talent and properly compensate our high contributors. These flexibilities will need to be considered as the National Security Personnel System is developed.

Other civilian initiatives include the recruitment of college students with critical S&E skills via recruiting incentives, a robust marketing effort, and a co-op central funding program that hires college students while still in school. Central funding for recruiting bonus and retention allowances for journeyman level S&Es also promises to provide much needed assistance with civilian recruitment and retention.

On the military side, we're employing the Airman Education and Commissioning Program and the Technical Degree Sponsorship Program to recruit additional S&Es into the military workforce. Bonus programs such as the Critical Skills Retention Bonus are essential to shrinking the current shortfall of military S&Es within the Air Force and the Air Force is currently exploring additional bonus programs.

The Air Force is committed to its S&Es and recently published a "Concept of Operations for Scientists and Engineers in the United States Air Force." We also baselined the requirement for the Air Force S&E workforce and, upon analyzing this baseline requirement, found that while our military and civilian authorizations were about right, our actual demographics were seriously short in some key areas. As such, we are shifting our focus to retaining the workforce we have and infusing it with the vitality of new S&Es to meet tomorrow's need. During the next seven years, we are investing nearly a third of a billion dollars to support the retention and reshaping of our technological workforce. As we replenish our S&E workforce, we are providing career guidance and mentoring that will enable us to meet our 21st Century challenge. Initiatives, such as the special hiring legislation authorized by Congress in Public Law 106-398, which provides "DARPA-like" hiring authority to the Military Departments, should also produce positive results in shaping our S&E workforce. This authority has only recently been delegated to the Air Force,

but we are optimistic about its potential. And, again, we express our thanks to Congress for your continued support.

### ***MAXIMIZING OUR S&T DOLLARS***

We will continue to leverage technology to achieve new levels of combat effectiveness. Our strategy is to pursue integrated technology capabilities that support our warfighter's highest priority needs. We must also pursue the fundamental enabling technologies that will improve tomorrow's Air Force. As technological superiority is increasingly a perishable commodity, we work hard to optimize our S&T funding, by not only "inventing the future" ourselves, but also by speeding the introduction of new technologies to our warfighters.

One way of rapidly transitioning technology to the warfighter is through our Applied Technology Councils and the Advanced Technology Demonstrations (ATDs). The councils are composed of two- and three-star generals from AFRL, our logistic centers, our acquisition product centers, and our major user commands who formally prioritize ATD programs. We hold an Applied Technology Council meeting with each Major Command twice every year and have commissioned 34 ATDs that have transition funding. The Applied Technology Council process is extremely important in linking the S&T Program to both the system developers, the logisticians, and the operational user. This process facilitates technology transition to operational use and secures user commitment for resources to do systems design and development and fielding of the technology. Currently about fifty percent of our Advanced Technology Development (6.3) budget is committed to these ATD programs.

Since deployed technology may remain in use for decades, the Air Force S&T Program not only focuses on enhancing performance, but also on sustaining our fielded warfighter

capabilities. Emphasizing affordability from the very beginning through training of our management, and science and engineering staff, as well as through an in-depth review of technology development efforts, increases our potential to reduce the costs of technology early in the system development process and throughout a product's life cycle.

We maintain an excellent balance of military, civilian, and contractor expertise, which allows us to be very selective about investing in high payoff technological opportunities. We constantly seek opportunities to integrate Air Force planning and leverage our S&T funds by cooperating with other Services, Agencies, the private sector, and international partners. For example, we rely on the Army as the lead Service for defensive chemical-biological technology development. The Air Force also has strong inter-Agency efforts, such as our program in aging aircraft, which is focused on detection and management of corrosion and fatigue in aging structures. It is closely coordinated with the civilian aging aircraft research programs at the National Aeronautics and Space Administration (NASA) and the Federal Aviation Administration (FAA). Our partnership with the industrial and university research base is very strong. In fact, we outsource over seventy percent of our S&T funding. Finally, the Air Force is involved in international cooperative technology development efforts for S&T, such as the software defined radio development, insensitive high explosives, and aircraft battle damage repair efforts conducted with the United Kingdom among others. Another example of international cooperation is the multi-domain network management program with Australia and Canada. This program is developing the concepts and tools for creating and managing secure computer networks with our coalition partners.

## ***WORLD CLASS RESEARCH***

The quality of our program is assessed by the Air Force Scientific Advisory Board (SAB) through yearly reviews. The SAB conducts an in-depth review of half of the S&T Program each year, covering the entire program over a two-year period. Twelve technical areas have been identified as world class research during the last cycle of reviews -- let me highlight a few of these areas that were identified as world class.

The Directed Energy Directorate's Starfire Optical Range at Kirtland Air Force Base, New Mexico, is leading the adaptive optics research for use in large ground-based telescopes to image satellites and propagate laser beams through the atmosphere. This will enable high-quality, ground-based observations of space objects and propagation of laser beams through a turbulent atmosphere. Astronomical images using this technology can rival those obtained with the Hubble Space Telescope.

Our Propulsion Directorate's Hypersonics Technology (HyTech) work at Wright-Patterson Air Force Base, Ohio, is acknowledged by the SAB as world class and a cornerstone of DDR&E's National Aerospace Initiative. Our HyTech program has continued to advance the state-of-the-art in scramjet engines and conducted the first ever ground test demonstration of a scramjet producing positive net thrust back in 2001. In February 2003, HyTech tested a flight weight scramjet Ground Demonstration Engine operating at Mach 4.5. While the 2001 Performance Test Engine used copper heat-sink hardware and weighted 1,500 pounds, the 2003 Ground Demonstration Engine used JP-7 fuel to cool the scramjet engine walls and weighed less than 150 pounds. This marked another first for the HyTech program—demonstrating the structural durability of a hydrocarbon fueled, actively cooled scramjet. Testing at Mach 6.5 is



currently ongoing and should be completed in April 2003. Pratt & Whitney developed this particular engine in collaboration with Air Force scientists and engineers.

Another SAB-rated world-class research program is the Warfighter Skill Development and Training efforts worked by our Human Effectiveness Directorate at Brooks City-Base, TX. Specific research areas include Integrated Panoramic Night Vision Goggle (PNVG) and Distributed Mission Training. The Integrated PNVG will improve situational awareness and terrain avoidance at night through its wider field of vision and improved resolution. It will also provide protection from laser target designators, laser rangefinders, and laser threats through compatibility with existing laser eye protection technologies. Distributed mission training will provide an integrated set of training, simulation, and mission rehearsal technologies that will improve warfighter capabilities and mission readiness by enhancing operator and team performance skills. Technologies will increase operational readiness by providing more effective methods and approaches to train and assess personnel. These technologies will contribute to a more highly trained and flexible cadre of personnel at a reduced cost.

Working closely with operational users, AFRL researchers in the Materials Directorate at Wright-Patterson Air Force Base, Ohio, continue to develop and transition new filter technologies that provide improved eye protection for aircrews from varied levels of laser threats. The Laser Eye Protection program is enabling aircrews to conduct day and night air operations without visual jamming or personal injury.

Our research in Electro-Optic Warfare at Wright-Patterson Air Force Base, Ohio, will allow future laser-based sensor systems to penetrate moderate cloud cover, obscurants, and camouflage. This will provide improved target detection and identification for our weapon systems. "See and Avoid" sensors will ease restrictions on unmanned air vehicle operations in

civilian airspace and allow autonomous operation in conjunction with manned aircraft. These technologies may also be applied as low-cost missile warning sensors to affordably protect military and commercial aircraft from surface-to-air missiles. Also, experimental research in infrared countermeasures is developing threat adaptive techniques for robust defeat of current and future infrared weapons and sensors.

Space Weather research at Hanscom Air Force Base, Massachusetts, is another SAB-rated world class operation. We have a strong modeling capability that specifies and forecasts space weather from the Sun to the ionosphere. Assessment capability of space environment and its effects using compact sensors will be incorporated into a high energy particles sensor that is under development.

At Edwards Air Force Base, California, the Propulsion Directorate is working on world class research in polynitrogen propellants. The goal is to enable high performance monopropellant rocket propulsion systems with revolutionary performance. By improving the specific impulse of the propellant, we will have environmentally benign exhaust and reduced signatures. This could potentially improve storage, manufacturing, and rocket engine size.

### ***COMBATING TERRORISM***

While the traditional focus of S&T has been on developing long-term capabilities, the Air Force S&T Program also contributes to the current needs of the nation and our troops deployed in hostile areas. One example of an Air Force project receiving a great deal of attention since 9/11 is the Elastomeric Coating polymer, which was developed by the Air Force to protect key buildings and installations from close proximity explosions, such as air dropped weapons or truck bombs. This easy-to-apply spray coating provides greater structural integrity of exterior

walls and prevents dispersion of debris as well as separation of wall elements. In addition to protecting lightweight shelters, this polymeric coating is currently being applied to the interior of the outer walls of the Pentagon.

Another transformational effort is the Vehicular Mounted Active Denial System (VMADS). The VMADS is being jointly developed with the U.S. Marine Corps and is a defensive millimeter wave system used for perimeter defense applications. It is a directed energy weapon that emits a non-lethal, non-damaging beam, which heats up the skin of a potential enemy when in close proximity to the system. The resulting temporary pain causes the person to flee.

In the war on terror, Air Force Special Tactics Combat Controllers are changing the very nature of warfare. By performing operations deep in enemy territory, they help determine who the terrorists are, where their weapons are located, and who the innocent civilians are. Then, they precisely control the elements of airpower to defeat the terrorist threat, while taking care to spare innocent civilian casualties and minimize collateral damage. Then, these same Special Tactics Combat Controllers are there to provide instant battle damage assessment. We call these deep engagements, "Battlefield Air Operations (BAO)."

The Air Force is accelerating new technology to these Special Tactics Warriors in the form of significant improvements to their BAO Kit of equipment. As a result of this Air Force enterprise, our Special Tactics Warriors will soon have a digital machine-to-machine capability that helps to quickly connect the right aircraft, with the right munitions, guided precisely to the right target, at just the right time, to achieve the desired effect. This new automated process helps to reduce the time it takes to target the terrorist threat, while at the same time reducing human error in the targeting process.

Working collaboratively with the Special Tactics Warriors, the Air Force "BAO TIGER TEAM" has also partnered with a national team of industry to field significant enhancements of increased capability, while reducing the weight and size of the individual BAO Kit equipment. They are performing these improvements by developing, prototyping, testing, building, and fielding these BAO Kit improvements in very rapid spirals. These new BAO capabilities will help to save American lives, and the lives of innocent civilians. BAO provides a revolutionary and highly effective way to combat the terrorist threat.

### ***TRANSFORMATIONAL TECHNOLOGIES***

There are many other Air Force technology areas that deserve special mention. Let me highlight just a few examples. As mentioned earlier, there's our transformational communications technology development program, whose laser communications technology efforts promise to increase data transfer rates at least ten-fold compared to current radio frequency communications systems. Additionally, laser communications uses a narrow beam, which decreases the likelihood of intercept and increases resistance to jamming. While laser communications have a high potential to revolutionize satellite communications, there are technical challenges to overcome such as precision pointing and tracking, weather constraints, and adapting the equipment for use in space. We continue to work on the technology challenges and are also conducting a study to determine the best architecture for implementing laser communications technologies to complement and integrate with radio frequency-based systems.

To increase aircraft survivability and operational efficiencies, the Air Force is developing both manned (F/A-22 and Joint Strike Fighter) and unmanned flight vehicles that can carry and employ weapons from both external and internal weapons bays. To increase the

number of weapons the flight vehicle can fit into their internal weapons bays, part of our investment strategy focuses S&T funding on developing and demonstrating smaller precision weapons.

One of the small munitions currently being flight demonstrated at Eglin Air Force Base is the Low Cost Autonomous Attack System (LOCAAS) technology program. The LOCAAS is a 100-pound class powered munition of which the primary target set is moving and relocatable targets. This Advanced Technology Demonstration (ATD) program will demonstrate the effectiveness and military utility of this type of munition for the Lethal Suppression of Enemy Air Defenses (SEAD), Theater Missile Defense (TMD) Attack Operations, and Armor/Interdiction mission areas. LOCAAS will integrate a laser radar precision terminal seeker with autonomous target recognition algorithms, a multi-modal warhead, Global Positioning System (GPS)/Inertial Navigation System (INS) mid-course guidance, and a miniature turbine engine with a fly-out range of 100 miles. This ATD program will complete five flight tests by the end of Fiscal Year 2003, culminating in a planned autonomous flight with active seeker and warhead against a real target. The first flight test was successfully completed on February 4, 2002, and demonstrated the powered flight envelope, GPS waypoint navigation, and simulated attack of a SEAD target. The second flight test, successfully completed on November 4, 2002, was a guided LOCAAS that demonstrated real-time autonomous search, and automatic target acquisition algorithms that could detect, identify, and simulate attack against a TMD target.

Plans are also being made in Fiscal Year 2004 to conduct a cooperative program with the Royal Australian Air Force (RAAF) using the LOCAAS vehicle. A test program on the RAAF F-111 aircraft in Australia is scheduled for the first quarter of the fiscal year. This will be an



important test for both nations -- the U.S. is able to test munitions release at supersonic speeds and Australia benefits from the test results. These results could enable maturation of the computational simulation codes for separation of symmetric and asymmetric miniature weapons, providing for a reduction in the risk and cost of weapons certification efforts for aircraft with internal weapons bays such as the F/A-22, Joint Strike Fighter, and unmanned combat air vehicles.

To continue the trend of miniaturization of space platforms, the Air Force and Defense Advanced Research Projects Agency (DARPA) have provided funding to ten universities to explore the military utility of innovative, low-cost nanosatellites. These nanosatellites, weighing two to ten kilograms, could demonstrate efforts such as differential GPS navigation, miniaturized sensors, and micropropulsion technologies. In December 2002, two "pico satellites" weighing slightly more than two pounds each, were successfully released from a specialized spring-loaded launcher assembly mounted on the sidewall of the Space Shuttle Endeavor. This was the joint Air Force/DARPA-developed PICOSAT Inspector experiment to demonstrate a significant step forward in the development of an on-board autonomous inspection capability.

The Air Force is also conducting the Experimental Satellite System (XSS) series to demonstrate increasing levels of microsatellite technology maturity. The XSS-10, the first microsatellite in the series launched on schedule during Fiscal Year 2003. It demonstrated semi-autonomous operations and visual inspection in close proximity of an object in space -- in this case a Delta II upper stage. In Fiscal Year 2004, we plan to launch XSS-11, which will demonstrate autonomous operations and provide experience with command and control in proximity operations to another space object.

One of the most transformational and quickly deployable technologies available today is command, control, and communications technology, also known as information technology. This technology is at the heart of our Moving Target Indicator Exploitation program, which is developing web-enabled automated tools to exploit data from current and future sensor systems such as the Joint Surface Target Attack Radar System, better known as JSTARS. The effort is focused on four technology areas: ground moving target tracking; motion pattern analysis; behavioral pattern analysis; and sensor resource allocation and scheduling, which provide the capability to track moving targets and get the information to the operations center.

### ***BREAKTHROUGH TECHNOLOGIES***

In recent years, we have all come to appreciate the success of unmanned vehicles. We hear over and over again the tremendous operational advantages that systems such as Predator and Global Hawk are bringing to warfighters from all Services. Over the first two decades of the 21st Century, advances in micro unmanned air vehicles will provide significant additional capabilities to our Armed Forces. Micro air vehicles utilize advances in microscale aerodynamics, electronic miniaturization, munitions, and propulsion to package sensory and weapons payloads into highly reliable, on-demand systems. These systems will provide unprecedented levels of situational awareness in the most severe threat environments. Whether we are operating in urban environments, sensing bio-chemical dispersion through the atmosphere, or looking over the next hill, our troops will have the awareness needed to fight and survive. These systems will provide the persistent intelligence, surveillance, and reconnaissance in high threat environments needed by our troops on the ground and our airmen in the air. When

called for, swarms of these vehicles will cooperate together to generate both lethal and nonlethal effects.

In the next 50 years, advancements in nanotechnology will provide the greatest change in how man operates since the invention of powered flight itself. Nanotechnology is a science and a series of disciplines that works at the atomic and molecular level to create structures, materials, and devices through improved molecular organization. By working with elements at the level of nanometer scale, we have access to the building blocks of nature. This will fundamentally change the way materials and devices will be produced in the future. The ability to synthesize nanoscale building blocks with precisely controlled size and composition and to then assemble them into larger structures with unique properties and functions will revolutionize segments of the materials and device industry. The benefits that nanostructuring can bring include lighter, stronger, and programmable materials; reductions in life cycle costs through lower failure rates; innovative devices based on new principles and architectures; nanosensors and nanoprocessors; and use of molecular/cluster manufacturing, which takes advantage of assembly at the nanoscale level for a given purpose.

Another significant breakthrough technology that will change the way we develop systems is our work in biotechnology. Biology has developed unique materials and processes that may be exploited in non-biological systems. We are studying the fundamental science necessary to incorporate biological components and organisms into Air Force systems. For example, in biomimetics, we research the adaptation of natural biological sensor in reptiles. The natural infrared sensors in reptiles do not need to be cooled. We hope to adapt this biological process to Air Force sensor applications that normally require cryogenic cooling.

## **TECHNOLOGY TRANSITION**

The majority of Air Force S&T is contracted with industry and universities. This promotes relationships between the scientists and engineers conducting the research and lays the foundation for technology transition. Strong connections between the technology supplier and the end user help speed transition of technology to the warfighter. In addition, the various transition programs in which the Air Force participates further cement this foundation. Air Force technology transition efforts include Advanced Technology Demonstration projects, Small Business Innovation Research (SBIR) contracts, and Cooperative Research and Development Agreements (CRADAs) among others.

The Applied Technology Councils discussed earlier were initiated in Fiscal Year 1999 to foster top-level user involvement in the transition of technology from the laboratory to the system developer to the operational user. As noted, these Councils review and approve Air Force Advanced Technology Demonstration projects and ensure that the Major Commands plan for the transition of successful technology by tying approved Advanced Technology Demonstration projects to planned Major Command Future Years Defense Program funding.

Another Air Force technology transition tool is the SBIR program, which funds early-stage efforts at small technology companies. These programs serve a defense need, but also have the potential for private sector and/or military market commercialization. A similar program, the Small Business Technology Transfer (STTR) program, funds cooperative efforts involving a small business and a research institution (i.e., a university), a federally-funded research and development center, or a non-profit research institution. Finally, a CRADA is an agreement between a government laboratory and a non-federal party under which the laboratory provides personnel, facilities, equipment, or other resources (but not funds) with or without

reimbursement and the non-federal party provides funds, people, services, facilities, equipment, or other resources to conduct specific research and development efforts that are consistent with the agency's mission.

These efforts along with many other programs, such as Dual-Use S&T, Independent Research and Development, Mentor-Protégé, Personnel Exchanges, etc., are mutually beneficial to the Air Force and the contractors and universities with whom we collaborate. Technology transition is a key component of the Air Force S&T Program and is vital to our pursuit of national security requirements.

### ***SECTION 253 STUDY***

Section 253 of the National Defense Authorization Act for Fiscal Year 2002, Public Law 107-107, directed the Air Force, in cooperation with the National Research Council of the National Academy of Sciences, to carry out a study to determine the effect of S&T program changes of the past two years. The Air Force Science and Technology Board (AFSTB) of the National Research Council will prepare a written report for the Secretary of the Air Force to forward to Congress by the May 1, 2003, deadline. While we do not have any insight into the AFSTB study results, we expect this study will reflect the positive impact of changes instituted by the Air Force in its S&T planning process.

### ***CONCLUSION***

In conclusion, the Air Force is fully committed to providing this nation with the advanced air and space technologies required to meet America's national security interests around the world and to ensure we remain on the cutting edge of system performance, flexibility, and



affordability. The technological advantage we enjoy today is a legacy of decades of investment in S&T. Likewise, our future warfighting capabilities will be substantially determined by today's investment in S&T. As we face the new millennium, our challenge is to advance technologies for an Expeditionary Aerospace Force as we continue to move aggressively into the realm of space activities. The Air Force S&T Program provides for the discovery, development, demonstration, and timely transition of affordable, transformational technologies that keep our Air Force the best in the world. As an integral part of the Department of Defense's S&T team, we look forward to working with Congress to ensure a strong Air Force S&T Program tailored to achieve our vision of a superior air and space force.

Mr. Chairman, thank you again, for the opportunity to present written testimony, and thank you for your continuing support of the Air Force S&T Program.

---

---

**QUESTIONS AND ANSWERS SUBMITTED FOR THE  
RECORD**

MARCH 27, 2003

---

---



### **QUESTIONS SUBMITTED BY MR. WILSON**

Mr. WILSON. All of us are concerned about friendly fire, fratricide, accidents, and the accident that occurred this week with the Royal aircraft and the Patriot-has there been any determination, even at this early stage, as to how that occurred or how that could be avoided?

Dr. SEGA. The Departments investigation into the Patriot friendly fire incident is still in progress. We will provide a briefing upon completion of the investigation.





# **FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT—UNITED STATES SPECIAL OPERATIONS COMMAND BUDGET REQUEST**

---

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ARMED SERVICES,  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES  
SUBCOMMITTEE,  
*Washington, DC, Tuesday, April 1, 2003.*

The subcommittee met, pursuant to call, at 2:00 p.m., in room 2212, Rayburn House Office Building, Hon. Jim Saxton (chairman of the subcommittee) presiding.

## **OPENING STATEMENT OF HON. JIM SAXTON, A REPRESENTATIVE FROM NEW JERSEY, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. SAXTON. The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this afternoon to consider the fiscal year 2004 budget request of the U.S. Special Operations Command. This will be an unusual hearing in several respects.

No combatant command, with the exception of Central Command (CENTCOM), is more engaged in Operations Iraqi Freedom and Operation Enduring Freedom than the U.S. Special Operations Command (USSOCOM). Special Operations Command (SOCOM) units are in combat, and SOCOM units will be needed to participate in the rebuilding of Iraq, and they are participating—as they are participating in the rebuilding of Afghanistan.

Unlike Central Command, which has forces provided by the services as needed, SOCOM relies continuously upon the same group of 46,000 troops that are a permanent part of the command. They are indeed intrepid warriors, and I am proud to say that they are American fighting men.

Because the command is at war, we have excused the commander and deputy commander from appearing before the subcommittee. However, since we are moving forward with our markup in early May, and since the fiscal year 2004 budget request for SOCOM reflects substantial increases in personnel, mission, and funding, we must, as the oversight committee, hold a public hearing on SOCOM's part of the budget request.

My colleagues know of my regard for special forces troops. I have visited all elements of special forces in recent months and have been uniformly impressed with the professionalism and patriotism found throughout the special forces units. The results of their efforts speak for themselves. Special forces have been brilliantly successful in Afghanistan and in Iraq. They are our nation's best weapon against global—the global war on terrorism.

The subcommittee understands that necessary wartime costs will be funded in the supplemental appropriation request now working its way through Congress. Nevertheless, the budget request represents a large peacetime, enduring commitment to a great number of special forces and resources. It is important for the subcommittee to receive testimony on these issues in open session.

While I believe that SOCOM units are our best weapon in the war on terrorism, I also worry that SOCOM units may be overused. I have heard repeatedly from senior commanders and understand from my personal observations of these fine men, that special forces operators cannot be mass produced. Members have also heard of problems with aging and overused equipment, particularly with aviation assets.

As a small, highly specialized, and highly trained elite force, there are never very many of these forces of any kind. Against that backdrop, and the temptation to overuse this force, I wonder what the long-term plan is, and look forward to hearing testimony on that point.

SOCOM, unique among the combatant commands, has statutory mission lists and special statutory procurement authority. The subcommittee will ask whether the mission list should be adjusted given the right emphasis on the counter-terrorism role, to find some other means to accomplish missions of lower priority. I am confident that SOCOM enjoys the special procurement authority, and the subcommittee will inquire as to how it is being used.

Our first witness is Marshall Billingslea, is the senior policy making office with the Department of Defense for special operations related matters. As such, he speaks for the command within the Pentagon and advises the Secretary of Defense of operations budgets, roles.

Before I welcome Mr. Billingslea, I would like to yield to my friend, Mr. Marty Meehan for any opening remarks that he may wish to make.

[The prepared statement of Mr. Saxton can be found in the Appendix on page 331.]

**STATEMENT OF HON. MARTY MEEHAN, A REPRESENTATIVE FROM MASSACHUSETTS, RANKING MEMBER, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. MEEHAN. Thank you very much, Mr. Chairman.

And I, too, look forward to receiving today's testimony and join you in welcoming our panelists.

SOCOM's position within the national command authority is indeed unique. Because of the foresight of individuals such as Congressman Daniels, Senators Nunn and Cohen, we have a flexible and operationally effective force well positioned to confront the challenges of terrorism and other asymmetric threats.

Long gone are the days that led to the 1980 debacle of Desert One where the equipment and unfamiliar units were thrown together in an attempt to rescue American hostages held in Iran. Today's special operators train extensively together and benefit greatly from improved acquisition procedures. Our nation is fortunate to have this arrow in its quiver.

That said, we are always looking for ways to improve. I note that the administration has proposed an expansion in the role of the command for combating terrorism. I see that the budget request proposals—proposes an increase in SOCOM's overall personnel end strength. And I am both heartened and intrigued by the newly proposed joint venture for leveraging SOCOM and Marine Corps assets.

If adaptability is a sign of the times, then kudos to both General Holland and General Jones for leading by example in prompting the respective establishments to adapt.

Mr. Chairman, on these and other issues, I look forward to hearing the testimony and I join you in commending our panelists. I would like to thank them for appearing and joining before us today. By working together, I hope we can continue to improve this unique and stellar organization.

Mr. SAXTON. Thank you very much.

We have two panels this afternoon. I would like to welcome our first witness, Mr. Marshal Billingslea, Principal Deputy Assistant Secretary of Defense for special operations, low intensity conflict.

Mr. Billingslea is acting as the Assistant Secretary of defense for special operations and low intensity conflict. At the outset I will state that without objection, Mr. Billingslea, your entire statement will be placed in the record, and we look forward to your testimony.

#### **STATEMENT OF MARSHALL BILLINGSLEA, PRINCIPAL DEPUTY ASSISTANT SECRETARY OF DEFENSE, SPECIAL OPERATIONS/LOW INTENSITY CONFLICT**

Mr. BILLINGSLEA. Thank you, Mr. Chairman, Mr. Chairman Congressman Meehan, members of the subcommittee, I appreciate your invitation to testify before the committee today on essentially three matters.

One, to update you on the progress we are making in prosecuting the war on terror, second to describe for you the strategy we are implementing today, and third to discuss the significant implications that strategy has for United States Special Operations Command, and Special Operations forces generally.

I do ask your indulgence today. We are in open session and I am not well-equipped to answer any specific questions regarding Iraq. So I am going to try to stay away from those issues to the extent I can, although I will try to provide a little context regarding the role that Special Operations forces are playing in Iraq and anything else I can take for the record and get answered for you as soon as possible.

Mr. SAXTON. Thank you.

We had the opportunity to meet with some Pentagon briefers this morning for a couple of hours on current operations, so we are in pretty good shape there, so thank you for mentioning that.

Mr. BILLINGSLEA. Thank you, sir. I will give you the bottom line at the outset of my testimony.

The United States and its allies have made significant progress in destroying and disrupting key parts of the international terrorist network with which we are at war. Al Qaida is an organization under great stress, with a leadership that seems increasingly less

able to plan multiple, large-scale attacks because they are focused on the more immediate problem of evading coalition capture.

I will add a qualifier, though, in a moment. USSOCOM has been a key player in that effort, and is working hand-in-glove with other parts of the United States government and with coalition partners.

The president's fiscal year 2004 budget initiates a significant transformation with USSOCOM into a supported combatant command for the war on terrorism. And it alleviates a number of mounting problems incurred by such a high op tempo for the command.

I mentioned a qualifier. I caution that today we are certain that we do not know all of the planning that al Qaida has already done, and we are concerned that they may have set in motion certain operations for the most recent chain of events that led to Khalid Shaikh Mohammed's capture.

Moreover, al Qaida and affiliated terrorist organizations have proven capable of regenerating lost parts and of changing tactics and techniques to adapt to our offensive efforts.

To put it simply, al Qaida and other related terrorist groups today remain intent on conducting devastating attacks against the United States, our friends and our allies.

At least some of their planning seems to contemplate the use of chemical or biological agents, in addition to their proven practice of using low-tech, conventional explosives to mount attacks with devastating consequences.

Before I describe the specific progress that has been made to date, I think it may be helpful to sketch out the nature of the international terrorist networks so that you can better see how we are targeting specific strands.

Al Qaida is perhaps best viewed as a spider web. At the center of the web are a number of terrorist groups, dozens actually, of varying sizes with varying agendas.

Al Qaida and its proxy groups, such as the IMU in Uzbekistan and Jamaah Islamiyah in Indonesia, and Abu Sayyaf in the Philippines and PIJ in Egypt, Algerian groups, such as the Salafist Group For Combat and Prayer, Chechen and other radical groups are part of this central part of the spider web.

From the core of the network tendrils around the globe. They reach deeply into those countries that the Secretary of State has termed state sponsors of terrorism.

I am talking about the Irans, the Iraqs, Libya, Syria, Sudan, Cuba and North Korea. The web stretches into ungoverned and less governed zones of the Earth, and the triborder area in Latin America, parts of Yemen and Pakistan and Afghanistan, and certain of the islands of the Philippines and Indonesia, parts of Lebanon, Somalia and other parts of Africa.

The web attaches itself to thousands of points; it reaches into foreign educational systems, the madrassa, is woven throughout certain religious institutions and has spread into non-governmental organizations and charities that are used as Trojan Horses to move people and finances around the world.

The tendrils creep into certain banks in the hawala system, and into various media outlets. They are also interwoven with other transnational webs.



There are linkages to drug smuggling, drug running rings, weapons smuggling and proliferation of weapons. The web reaches well into friendly nations. Nearly every NATO partner has uncovered one or more al Qaida cells.

In fact the terrorist network reaches right into our own backyard, to America. As the president mentioned in the State of the Union, Buffalo is but one city in which we have discovered al Qaida penetration.

The spider web of loosely organized terror groups has no single integrated command structure. While the leadership of some key organizations can be eliminated, those organizations do not necessarily cease functioning.

We have seen cells either continue to operate quasi-independently or begin to coordinate with either terrorist organizations. In some cases we found senior operational coordinators to be interchangeable with one another, meaning that they can and they do supplant one another in event of capture, and they persist in the execution of operations.

Likewise, these organizations, as I mentioned, are capable of replacing lost leadership by renominating or nominating operatives and elevating them in stature.

Obviously, key arrests have disrupted terrorist attacks, but there is a crucial difference between a suspended terrorist operation and one that has been truly abandoned.

Some of the groups in the international network, and al Qaida in particular, have proven themselves exceptionally patient and deliberate. We have seen instances where the planning for an attack was temporarily suspended after an arrest or a death, only to resume a few months later under different leadership.

Clearly, when faced with such an adaptive organization we cannot apply pressure sporadically or unevenly. It has been necessary for us to engage quite literally in a full-court press, bringing to bear all elements of our national power.

Striking at this network has necessitated an unprecedented level of cooperation among U.S. defense, intelligence, law enforcement and diplomatic agencies.

Likewise we are benefiting from and are part of an unparalleled level of cooperation on the global scale between departments and agencies of numerous foreign governments, acting both in concert with the United States, with one another and on their own.

There is truly a global coalition against terrorism, and that coalition has had some successes which I will now describe.

The groups that are today conspiring to commit mass murder of American and allied citizens operate overtly out of a handful of terrorist sanctuaries.

The United States government is systematically draining those swamps in a denial-of-sanctuary campaign. Afghanistan was the first such territory, post-September 11<sup>th</sup>, that the United States liberated from the grasp of a terrorist organization.

In losing Afghanistan, al Qaida lost its ability to continue using the enormous two-decades old infrastructure of paramilitary training camps that were scattered throughout that country.

The loss of these camps had an immediate and obvious impact on al Qaida. Gone were the training facilities, chemical and biological



cal research laboratories they created, along with some of the equipment they had procured.

The leadership was scattered and trustworthy communications became much, much harder to have. But the loss of Afghanistan also has had a deeper, intangible affect on terrorist organizations, a little harder to describe.

There no longer is an equivalent place where aspiring young terrorists can go with one another to bond and demonstrate their commitment to fundamentalistic extremism and to receive a rigorous physical and operational regiment.

The psychology of the Afghan terrorist camp network, luckily for us, cannot be easily replicated. With that said, al Qaida and others are trying, and they are finding sanctuary in other countries. Iraq is one such place. We are now in the process of denying al Qaida and other terrorist groups sanctuary in that country, and we are cautioning other nations not to allow al Qaida across their borders or to operate within their territory.

At a very early phase of the campaign in Iraq, the United States struck multiple terrorist training facilities in the northeastern part of that country. Secretary Rumsfeld has noted those initial airstrikes were then followed by operations on the ground by Kurdish forces. The targets are a network of facilities run by an extremist Kurdish organization called Ansar al Islam. Those camps have become over the past year and a half, a safe haven to several al Qaida operatives and a home to part of al Qaida's chemical warfare program.

In the months prior to Operation Iraqi Freedom, the Ansar camps had swelled with foreign fighters seeking an opportunity to conduct terror attacks against the United States. We believe this happened with the knowledge and/or complicity of the Iraqi government.

It is difficult to say at this stage how much damage has been inflicted on Ansar al Islam and al Qaida in Iraq, but there is a concerted push underway. You may have seen this morning's press reporting out of Italy where an Ansar cell allegedly has been rolled up. In total, we believe there to be more than a dozen terrorist organizations operating from sanctuaries in Iraq. Our goal is to eradicate their presence from that country.

Denial of sanctuary is but one aspect of the campaign. Degrading terrorist finances also is crucial since it translates into a degradation of operational capability. The United States government has taken steps to freeze the assets of, block travel by, and to criminalize relationships with 36 different foreign terrorist organizations; 60 entities have been listed under the Executive order, 48 groups designated pursuant to the USA Patriot Act.

It does not take a great deal of money to conduct terrorist operations. Tens of thousands of dollars or even hundreds of thousands are not necessary or are often all it takes to spin up a cell to commence operational planning. That is why the freezing of more than \$100 million in terrorist finances is so significant. Equally important, we have been able to identify several key terrorist financiers and to take steps against them. The al Qaida financier, Al-Hawsawi, for instance, has been captured as our key couriers in al Qaida.

The United States and coalition partners also have made progress in systematically reducing terrorist rank-and-file and in capturing or killing terrorist leadership and senior operational planners. Since September 2001, more than 55 terrorist leaders and planners have been captured or killed. In the past six months alone, there have been more than 30 arrests and seizures in 20 different countries, not counting ongoing U.S. military operations.

Two prominent al Qaida, Muhammad Atef and Abu Ali al-Harithi, have been killed. Several other prominent operatives, such as al-Nashri, Abu Zubayda, Ramzi bin al shibh, al-Libi and al-Jazair, are in custody. And of course, the terrorist that we believe was the mastermind of the September 11 attacks, Khalid Shaikh Muhammad, is now under coalition control.

Khalid Shaikh Muhammad's arrest is only the latest in a string, following January's arrest by Spanish authorities of more than a dozen terrorists, along with significant weapons caches found; and the February arrests in Italy of more than two dozen al Qaida sleepers. Khalid Sheik Mohammed's arrest, in turn, was followed by the March 2003 captures of al Qaida operatives reported in Africa.

And when you add to this previous progress made in destroying part of the al Qaida Poisons Network through arrests in London, Paris and Spain, and some of the progress that has been made in the United States with several of the arrests in key cities. You have seen an organization that we hope is feeling the affects of our combined efforts. Jemaah Islamiyah (JI), a terror group closely tied to al Qaida, also is under strain. There has been an unprecedented level of cooperation between the nations of southeast Asia in destroying this network.

In the past six months, Singapore has rolled up at least 21 JI members, Indonesia has arrested the senior JI spiritual leader, Abu Bakar Bashir, the JI operations chief and a senior member. There have been other key arrests in Malaysia, Thailand and the Philippines, although a key JI figure, Hambali, is still on the run. I could go and link other groups that comprise parts of the international terrorist network, but I will leave at that. My written testimony—

With respect to terrorist cadre, the foot soldiers and the cell members, more than 3,000 operatives have been captured in over 100 countries by the international coalition. The United States itself, today, detains at Guantanamo Bay nearly 700 enemy combatants, including operatives and mid-level planners encountered on the battlefield. These enemy combatants are being questioned for information they hold regarding planned future terrorist attacks. The information they are providing has enabled us to better understand the nature of the global terrorist network, how key organizations operate, build cells, move money and people, recruit individuals, and thus is helping us to dismantle these groups.

Based on their information and that extracted from sources under foreign control, the U.S. has been able to disrupt, or cause to fail, more than a score of planned attacks.

Failed and/or disrupted terrorist attacks have run the gamut in terms of target and venue, and scope, ranging from the dirty bomb, radiological dispersion plan against the United States, to plots in

Italy, London, France, Germany, Colombia, Israel, Singapore, Morocco, Russia, Indonesia, the Philippines, Spain, and Turkey, only to name only a few.

At this stage, I will also highlight the fact that the United States, working with key coalition partners, has been able to disrupt and avert a string of terrorist activities being orchestrated by the Iraqi Intelligence Service using terror groups as proxies. For instance, in the Philippines, the Abu Sayyaf Group publicly announced the financial support it was getting from Iraq to conduct terror attacks against U.S. nationals.

You may have noticed the large number of Iraqi nationals being evicted or arrested worldwide. We do not know the extent to which we have stopped Saddam's operatives from mounting terror attacks, but we certainly have thwarted some of their plans.

That said, the United States and its coalition partners have not been able to prevent key terror attacks. Jemah Islamiyah's bombing of the Bali resort killed more than 200 innocents, including seven Americans.

Despite several seizures of car bombs by Colombian authorities, the Revolutionary Armed Forces of Columbia (FARC) recently executed a bombing against a club in Bogota, which killed 34 and wounded 150. Similarly, the bombing of the synagogue in Tunisia, and the attacks on the hotel in Kenya and the El Al flight, are examples of operations that we were not able to avert.

Moreover, some groups have adjusted their planning to account for our efforts, and have gone small and local. The assassination of Lawrence Foley, a USAID employee, is an example. Others include the bombings launched by Abu Sayyaf in the Philippines, and the targeting of U.S. Marines by terrorists in Kuwait.

And, as I said at the outset, we know that al Qaida and other groups continue operational planning for significant terror attacks, and may have some plans nearing the execution stage.

That brings me to an important point. The war on terror has come at great cost to the American people, and our losses on September 11 were not the last of it. Since that time, a number of American patriots have given their lives in service of the nation. Several U.S. departments and agencies have lost people; I mentioned Lawrence Foley. The Special Operations Community, in particular, has lost several of its best and brightest. To date, there have been 137 SOF wounded, 91 of whom sustained injuries during combat. Thirty eight, Special Operations Forces (SOF) have been killed in the course Operation Enduring Freedom and related counter-terror missions.

For the Department of Defense, U.S. Special Operations Forces are at the tip of the spear in waging war against terrorism. One of the first blows struck in Afghanistan was the fight to topple the Taliban and deny al Qaida sanctuary. On the ground, less than 500 Special Forces personnel mounted an unconventional warfare effort, tied closely to indigenous forces and linked with the United States Air Force in a way that provided for a rapid, decisive, and crushing defeat of the Taliban's conventional forces.

The operation in Afghanistan was prosecuted by small units that operated with autonomy in a highly fluid environment. It was won by people who could and did meld with friendly Afghan forces, who



were willing to operate without a safety net; willing to develop such a rapport that they could trust their own security to their Afghan allies; live without a huge logistics train to provide equipment and supplies; be able to distinguish between combatants and non-combatants in an environment where civilians and fighters, Taliban and non-Taliban, and ex-Taliban, were all jumbled together and able to engineer combined arms operations between U.S. B-52s and the Northern Alliance's Soviet era tanks.

A myriad of SOF capabilities were demonstrated during Operation Enduring Freedom. While Army Special Forces conducted unconventional warfare with the Northern Alliance to destroy the Taliban's war fighting capability, other Army and Navy SOF were conducting special reconnaissance and direct action to destroy Al Qaeda. Army Rangers demonstrated their strategic reach during night operations. The Air Force and Army special operations aviators performed their work under incredibly difficult circumstances.

Most interestingly, Air Force Special Tactics airmen transformed the role of SOF by integrating every U.S. service's air power into the operation. Their unique ability to rack and stack multiple kinds of aircraft, procedures, and communications frequencies and to bring precision dumb ordnance danger close and on target proved crucial to halting and reversing Taliban offensives throughout the countryside, and ultimately to crushing the resistance around key cities. The result of this combined push by SOF was a Taliban uprooted and an al Qaida on the run.

Other SOF capabilities have assumed a newfound importance. We all have heard the term winning hearts and minds. SOCOM's Civil Affairs men and women are deployed worldwide long before hostilities erupt. And they also remain long after the guns have fallen silent to help rebuild the instruments of effective governance.

The work of Civil Affairs in Afghanistan sends an important message to the Muslim world. Our quarrel is not with Islam. Our fight is with terrorists and those who support or harbor them. By removing the Taliban, we have made life livable, once again, for the Afghan people. And the same will be true for the people of Iraq. It already is the case in the southern part of Iraq today, as humanitarian aid has begun to flow in.

The success of our Civil Affairs people, tied to a message that the Muslim world needs to hear and understand.

Which brings me to another invaluable part of the Special Operations Community, the servicemen and women of the Psychological Operations Detachments. These people are spearheading U.S. efforts in a war of words and a battle of ideas. And their success also is fundamental to our victory in the war on terrorism.

Now, despite the fact that SOCOM was deeply committed to the Afghanistan theater, in support of U.S. Central Command (CENTCOM), the command proved that the United States could mount other major SOF-run operations concurrent with, and shortly following, Operation Enduring Freedom.

Today, with Special Operations Forces heavily committed in Iraq, there nevertheless are concurrent operations being run in Afghanistan, Yemen and the Horn of Africa, and SOF advisers scattered throughout numerous other countries conducting indigenous train-

ing and facilitating the flow of tactical information for host-nation run efforts.

Having said all that, we are learning a number of lessons from the war on terrorism. And we have begun a significant retooling of the U.S. Special Operation Command (USSOCOM) to enable the command to lead the war effort in an even more effective manner. Congress will see that re-engineering effort manifested in the president's fiscal year 2004 budget request.

Perhaps the most important of these changes is a shift in expectation by the department that USSOCOM will no longer serve as primarily a supporting command, but rather will plan and execute key missions as a supported command.

That change from supporting command to supported command will necessitate some significant funding changes and the addition of certain types of personnel and units. Additionally, USSOCOM will look to move beyond certain collateral SOF missions, either in part or perhaps in full, to conventional branches of the military in order to free up special operators for their primary mission, which is to wage war against terrorists.

In the president's budget for fiscal year 2004, an increase of about 47 percent has been proposed for USSOCOM. That totals approximately \$4.5 billion. This increase includes an additional \$391 million for operations and related expenses, and about \$1.1 billion in procurement of critical equipment.

These increases facilitate the addition, as Congressman Meehan mentioned, of about 2,563 more personnel in critical mission areas. Military personnel costs, which are included in the budgets of the military departments themselves total another \$1.2 billion.

Some of the increase in funding will allow SOF to forward deploy into, and sustain operations in, areas where terrorist networks are operating. Additional funding also is devoted to investments in critical low-density/high-demand aviation assets that provide SOF with the mobility necessary to deploy quickly and execute missions effectively.

We are going to fix command and control shortfalls in both equipment and personnel. Provide USSOCOM with both a strategic planning and operations capability for missions launched from the United States. And also to run operations via the various several theater Special Operations Commands who are now dual-hatted, with responsibilities to both the regional combatant commander and to USSOCOM.

In addition, several of the Theater Support Operations Cells (TSOCs) will receive additional personnel and equipment to support the continuing war-level pace of activity in various theaters. For example, we plan to begin forward basing of additional SOF units and mobility platforms in CENTCOM. That includes Navy SEAL teams and Army and Air Force SOF aviation units.

Although I caution that specific basing decisions have not been finalized. In total, the TSOCs, the theater Special Operations Commands, will receive 232 additional personnel and additional command and control and communications equipment.

Also, we are allocating funding to sustain equipment that was acquired in the fiscal year 2002 supplemental. Some additional equipment and sustainment costs associated with transfer of personnel



from the service departments to USSOCOM are also going to be covered by the funding increases.

In terms of equipment, several critical equipment acquisitions are being put into motion with the 2004 increases. The budget will mitigate a shortage of critical aviation assets, including through the life extension and modification of existing platforms. Specifically, USSOCOM will begin modification of 16 additional CH-47s into MH-47Gs.

We will fund an MH-60 service life extension program to improve the avionics and give those airframes another 20 years of life, accelerate the MC-130H aerial refueling platforms, continue the modification of 4 C-130s into AC-130U gunships, and weapons kits and ammunition for 10 additional MH-60 Defensive Armed Penetrators.

I will note that the MH-47E has proven a workhorse in offensive combat operations, but that the handful of available platforms have taken a beating. More than half of the MH-47 fleet has been destroyed or damaged at some point. And there is a great deal of tired iron in the USSOCOM inventory at this stage.

When you measure your assets in ones and twos, or even 10s, as USSOCOM does, the loss of a single system can have far-reaching effects. Fixing USSOCOM's mounting aviation problems that are accruing simply due to the high OPTEMPO of counter-terror operations is a top priority within this budget. And because we know to expect future loss of systems and platforms, we have begun planning an attrition reserve for the command.

There is additional funding which allows procurement of new capabilities. The 2004 budget begins a long overdue modernization of psychological operations (PSYOP) media production, broadcast, leaflet delivery systems and so forth.

U.S. PSYOP capabilities have, in our view, proven their worth in Afghanistan, and now in Iraq. And we are going to capitalize upon the recent revolution in telecommunications technology by providing the command with a research and development program to demonstrate the utility of certain technologies such as satellite radio and UAVs for PSYOP messages.

As far as the people, I mentioned earlier in my testimony the exceptionally high caliber of individual who serves as a SOF operator.

Mr. SAXTON. Mr. Secretary, could you just kind of hit the high points within the rest of your testimony?

Mr. BILLINGSLEA. Absolutely, sir.

Mr. SAXTON. Thank you.

Mr. BILLINGSLEA. The bottom-line on this is that we are going to propose an increase of 2,563 personnel in fiscal year 2004. The adds for the TSOCs and increases the shooters and others. Civil Affairs increases and PSYOP increases.

I can address transition of missions to non-SOF forces and the extent of the new relationship that we are building with the U.S. Marine Corps if members are interested.

With that, I will wrap up and I will answer any questions you may have.

[The prepared statement of Mr. Billingslea can be found in the Appendix on page 335.]

Mr. SAXTON. Thank you very much.

Well, as I said in my opening statement, your participation here is very much appreciated, and you are very thorough on a summary of what has been happening is also much appreciated. I am going to save my questions for last.

Mr. Meehan, would you like to lead off here?

Mr. MEEHAN. Thank you, Mr. Chairman.

Mr. Billingslea, the administration has proposed a—as we are discussing, a new role for SOCOM that would involve additional planning and staffing. It seems to me that this new role of the supported command will require consequential increases in the demands placed on the intelligence community. Given this, how are you working within the DOD with the intelligence community to alleviate this additional requirement? And I was wondering if there are any specifics that you could enlighten the subcommittee on in this regard?

Mr. BILLINGSLEA. There are a number of changes that are either proposed or underway to address this issue. But the command itself is as constructed planning and intelligence fusion capability that is being stood up and further augmented not only by intelligence personnel, but by planners from the other combatant commands and from other agencies as well, the Department of State and others.

The Defense Intelligence Agency has made a number of changes to give the kind of analytic focus on counter-terrorism operations that the command needs. That change has already been accomplished. And this is very much a matter of concern and a matter of focus for the new under secretary of defense for intelligence, Dr. Steve Cambone. I can pass further information forward, maybe in a classified channel, to further address that.

Mr. MEEHAN. Great.

Also could you please share with the subcommittee the department's latest view on the use of special operations personnel for humanitarian de-mining activities? Our efforts in Afghanistan, obviously, have been affected by the number of combines in that country. What are the pros and cons for using SOCOM personnel for those kinds of missions?

Mr. BILLINGSLEA. I know for a fact that we look at those kinds of missions on a case-by-case basis. It is not necessarily a case that SOF assets should be used for de-mining in each and every instance. But there are times and places where you would want to employ SOF to do that, and this is an area where the civil affairs folks, in particular, and SOF folks in terms of mine awareness campaigns.

There are some very unique capabilities resident in those communities. In a place like Afghanistan where security is always a concern, and so, you do need to have an organic force protection capability. You may find that your de-mining mission really ought to be not done by, but overseen by U.S. personnel, maybe civil affairs or others. I would just say we take it on a case-by-case basis.

Mr. MEEHAN. Thank you, Mr. Chairman.

Mr. SAXTON. Thank you.

Mr. Kline.

Mr. KLINE. Thank you, Mr. Chairman.

And thank you, Mr. Billingslea, for being here today, and for your testimony.

I have got a question around the concept of the group operation that is going on between the United States Marine Corps and SOCOM. I guess my concern is that the Marine Corps is not a very large service. How do you see this developing? And does this open up the possibility of drawing hundreds or thousands of Marines into this rotating detachment?

Mr. BILLINGSLEA. I do not think that is the plan. Obviously, we will continue to all watch this very closely from both sides of the equation. I personally believe that it is evolving in a very healthy direction at the moment. I mean, for the first time in history you have got collaboration, you have got the beginnings of a construct for joint warfighting between the command and the Marine Corps.

The detachment itself is only 85 Marines, and it just activated in March, and they are going to go through extensive training, and they are going to deploy with naval special warfare squadrons next April. At this time, it has seen as an augmentation of the plan is not to begin to rope such large numbers of Marines.

Mr. KLINE. I am struck by your comment that for the first time there is a construct for joint warfighting between the Marine Corps and the Special Operations Forces and SOCOM. In my memory, which is a little bit clouded today, it seems to me that Marines have been working with SEALs and SOCOM units for a long time.

The Marine Corps has had a Marine Expeditionary Unit Special Operations Capable program for many years where I thought we had been working together—Marines and Special Operating Forces—so I am not sure that I understand the notion that they have not had some mechanism for working together in the past. Am I missing something here.

Mr. BILLINGSLEA. No, sir. In fact, I think we are probably both saying the same things with just different terminology. This is more of a formal Title 10 delineated kind of structural integration that is happening here. It is more of a proof of concept at this stage than—

Mr. KLINE. So this is actually using Marines as Special Operations Forces as we use Army and Navy and Air Force personnel specifically in that category, and that is my understanding as well. I just wanted to get clear in my own head and in the minds of my colleagues here in the committee that the Marines working with the Special Operations Forces is not new.

Mr. BILLINGSLEA. Absolutely.

Mr. KLINE. What is new is incorporating them as SOCOM forces themselves. And again, my concern would be that if we press that very hard, then we are going to have to look at the overall end-strength of the Marines and SOCOM if that is going to grow to any significant size. And you are suggesting that it is not, that we have got an 85 Marine detachment.

Mr. BILLINGSLEA. I think we want to let this thing evolve and not put any definitive expectation on the end result of manpower. This has implications not just for the Marine Corps, but also for U.S. SOCOM and its resources. So we are going to just let this thing evolve from a prudent concept at this stage and see where we wind up here.

Mr. KLINE. Okay. I am interested in how things evolve in manpower issues, but I take your point.

Mr. Chairman, I yield back.

Mr. SAXTON. We are going to go to Mr. Lobiondo next, but while we are on this subject if I can just make two points and then a question on this subject.

Recently my nephew completed his basic training at Parris Island, and while I was there had the opportunity to talk to the commanding general. I learned that their rate of graduation from the time a group goes in, on average, they graduate 97 percent of the people.

A few weeks later I was in Coronado, where the SEALs, whom you have mentioned, do their basic training, and I was told that they graduate 20 percent of the people who started the class. Which means that the end product is likely very different among SOF forces, especially the SEALs, with whom these marines are going to deploy.

And so, I think it is good that the process is a process that is going to evolve because I am not sure, based on talking to marines and SOF—people who are a lot smarter about SOF issues than I am—how these two levels of training, if you will, mesh together.

And I also know that there is—this is a second observation and what raises questions in my mind about how this evolution will take place—is that the Marine culture is a very proud culture, but is a very special kind of culture that recognizes its ability to do a very special mission. SOF culture is a different culture and trained for a different mission.

And so, there are those two kinds of questions that really trouble me about how all this is going to evolve, and I guess I would just like to ask you for your perspective.

Mr. BILLINGSLEA. Sir, I think you have put your finger on the fact that we are bringing two very proud cultures with very different abilities together and integrating them.

With that said, I would say when you look at the Special Operations Command and you consider some of the differences between the SEALs and the rangers and the other special forces, Air Force, it is a mix of different kinds of people at different stages in their careers who come into the command with different levels of training, different levels of maturity and language skills and all of these different assets. And so, there is a wonderful opportunity to see this relationship with the Marine Corps move forward.

In fact, to move it forward within Special Operations and Low Intensity Conflict (SOLIC), within the policy side, the civilian side of the House—we had a one-star Marine general, who has now moved out of SOLIC and gone down to be chief of staff at U.S. Special Operations Command to help with this integration. I feel very good about where we are today.

Mr. SAXTON. Thank you.

Mr. Lobiondo?

Mr. LOBIONDO. Thanks, Mr. Chairman.

Mr. Secretary, thank you for being here.

The department has asked for legislative authority to use counterdrug funding for counterterrorism operations in the South-



ern Command area of operations. Could you tell the subcommittee a little bit about the reason for this request?

Mr. BILLINGSLEA. Yes, sir.

That is a Southern Command (SOUTHCOM) request, and so I am going to defer on giving you a concrete policy answer right now. What I will tell you is that within not only SOUTHCOM, but worldwide we have seen a nexus between drug-running and terrorist groups. When you look at organizations such as al Qaida, the drug-running activities are there as a method of containing finances.

Other groups, like Abu Sayyaf, are even much more heavily into the drug smuggling. And then you get all the way down to a group like the FARC in Colombia, where they are, in essence, a narco-terrorist organization.

So a distinction between narcotics trafficking and other trafficking activities by terrorist groups may be a bit of an artificial distinction, and it does seem to the department that if you are going to pursue efforts to dismantle narco-terrorist groups, then you want to pursue efforts that not only focus in on the drug smuggling, but also the weapons supply chains, the financial chains, the personnel and logistic chains as well to enable you to dismantle those organizations.

So I cannot speak for SOUTHCOM, but I would suspect that that is the logic behind their request.

Mr. LOBIONDO. Thank you. One more question, Mr. Chairman.

Are there any missions that SOCOM now performs that you believe should be performed by regular forces?

Mr. BILLINGSLEA. There may well be. I do not have any to propose specifically today. We are taking a look at that. There is a sense that there may be not wholesale divestiture of missions. A lot of this is written in the statute, and so you would not do this without talking to Congress at great length. But there may be certain missions for which U.S.

SOCOM should always be the command approached to do something, that maybe these missions could be performed by others and, in fact, quite frequently are performed by others—conventional side of the military. And so, what we are doing is a top-to-bottom review, and what is motivating this is if nothing else, trying to get some of the operations tempo (OPTEMPO) strain off the SOF operators who—the OPTEMPO pressures are very high.

Mr. LOBIONDO. Thank you, Mr. Chairman.

Mr. SAXTON. It is just interesting to note on Mr. Lobiondo's very good question that part of Section 167 of the appropriate statute delineates the areas of special ops activities. And so, we would look forward to working closely with you if they are going to be any major changes suggested relative to those activities.

Mr. BILLINGSLEA. I need to tell you right at the outset, Mr. Chairman, we are not asking at this stage for a change in Title 10 or any other statute related to U.S. SOCOM.

Mr. SAXTON. Mr. Hayes.

Mr. HAYES. Thank you, Mr. Chairman.

Just to start, Mr. Billingslea, thank you for your very concise, accurate and thorough testimony. And, Mr. Schulte, behind you, has



assured me that any aviation assets that you need, just give him a little money, he will be sure and get them quickly.

Going from a supporting to a supported command, tell the committee how that is going to improve. I agree that that is a good plan. Elaborate on how that is going to help you prosecute the mission better.

Mr. BILLINGSLEA. It will enable one command to be singularly focused on the task at hand of identifying, capturing, killing key members of terrorist organizations. The regional combatant commanders have not only that duty within their regional purview, but they also have a variety of other security responsibilities managing the U.S. footprint in various countries as it relates to the broader nation state dynamic.

So U.S. SOCOM has been tapped as being singularly devoted to the counterterrorism mission. Making them the supported command, in effect, brings with it not only the resources, but the responsibility for identifying and executing operations in various regions and gives them the ability to tap into regional assets under the command of regional combatant commanders to pull off those missions.

Mr. HAYES. Planning, as well as reactionary, in other words.

Mr. BILLINGSLEA. Hopefully less reaction and more—

Mr. HAYES. Exactly.

So more flexibility and ability to use available resources is also part of what I hear you saying.

Mr. Chairman, interestingly, we watched a Marine urban terrorist exercise and part of the information we have is the Marine Special Operations folks are 23 years old and our Army guys are 27, on average, across the board. We are going to have to have—or we have funding for 2,500-plus additional special operators. I have tremendous respect and pride in all our military, but from your perspective, how do we find an additional 2,563 special operators and get them into the system prepare them?

Mr. BILLINGSLEA. Well, through a variety of mechanisms. Also, we are focused on retention as a major objective. I think that there are a couple of things we can do; maybe a reduction in U.S. naturalization time could increase the number of potential recruits; the Army began an off-the-street recruiting program for special forces and the results to date have been very, very good; the U.S. Navy has relaxed some of the visual requirements for SEAL candidates to increase the number of available recruits.

There have been some low pipeline graduation success rates. That has hampered the ability of the services to train up some areas through back-fill losses, but we have seen an increase in fiscal year 02 retention due to various stop-loss programs and other measures. So we feel relatively comfortable where we are on the recruiting and the retention track.

Mr. HAYES. And it is safe to assume that anything this committee can do to help you recruit and supply these assets you will let us know?

Mr. BILLINGSLEA. Yes, sir.

Mr. HAYES. Please talk about the Osprey for just a minute related to if it were in the field, ready and operational, and please tell

us some of the things it could be doing for us today in Iraq. And how do you feel about the program today, given the need for it?

Mr. BILLINGSLEA. Well, the plane itself is still in the testing and evaluation stage. As you know, the command is greatly interested in the Osprey because of the carrying capacity and the operating range that it offers. So we are continuing to plan for and hope for the success of that platform.

There are all kinds of what-if's that can be asked. What if it does not prove out? What if there is another problem? We are going to hope against that. And there is some contingency planning, but I really would rather not get into that just yet.

Mr. HAYES. Probably a little bit of an unfair question, though. I know your aviation diagram and I can see, given the distances in the mission in Iraq, that that kind of speed and that kind of ability to get in and out quickly and load carrying in high altitude would be a tremendous asset. Thank you for your testimony.

I yield back, Mr. Chairman.

Mr. SAXTON. Mr. Rodriguez.

Mr. RODRIGUEZ. Thank you, Mr. Chairman.

Let me first of all thank you for being here. And I just wanted to ask, real briefly, when it comes to the force protection in terms of both chemical and biological weapons, where are we on that? Do they have the technology that is needed by now? Because I know that, you know, there is nothing worse than to have some of that available and then not being able to have access to it.

Mr. BILLINGSLEA. Yes, sir, there is a robust capability. That actually is something the Marine Corps excels at in particular. That is an organic capability for conventional military units as well as a capacity that U.S. SOCOM has for its individual aims with some very specialized capability.

There also is deployed overseas right now for Iraq a task force that is specifically devoted towards chemical and biological protections and radiological for U.S. servicemen that also are prepared to offer assistance to the Iraqi people if something should happen there. It is difficult to plan against because you are planning against a variety of unknowns. But we planned to the best of our ability.

Mr. RODRIGUEZ. On the 2,500 number, how many—I do not want you to tell me specifically, but how many of those would actually be able to go out in the field?

Mr. BILLINGSLEA. The short answer is the majority of that number would, but it has spread across a variety of different capabilities like civil affairs—a lot of that is civil affairs units, SOF capabilities. There are some combat capabilities in there, and there is also a small amount of personnel in-strength devoted to head-quarter staff; the planners, the operational planners—

Mr. RODRIGUEZ. Because in all honesty I think this is the area where we really need to keep up on, and that sounds even like a smaller number than what I would have thought, especially going after, you know, terrorists. I think that is the area that we have got to keep up with. We have not been too good at going after drug gangs, we have not been successful there and this is very similar.

Mr. SAXTON. Thank you.

Mr. Joe Wilson, the gentleman from South Carolina.

Mr. WILSON. Thank you, Mr. Chairman.

Thank you very much for being here, and it has been very encouraging for me to hear the operations that you are conducting. It is so important to me that the terrorists be stopped overseas before they get here. And so, anything that I can do to assist our very able chairman here to back you up I want to do it.

I was interested in particular your reference to Ansar al Islam and the facilities that they have been running in Iraq. It is been somewhat confusing to me because on the maps it looked like to me that the training facilities were in the Kurdish-run area of Iraq, and would that still be directly responsible to Saddam Hussein or not? Or how do we directly relate that to Saddam Hussein?

Mr. BILLINGSLEA. Those camps, sir, are in the Kurdish area. Ansar al Islam is—

Mr. WILSON. Extremist Kurds.

Mr. BILLINGSLEA. Well, it is an extremist Kurdish group, yes, sir. But that is an area controlled by Baghdad. It is not in the no-fly zone. Control is an interesting term in Iraq, but Saddam is the sort of despot who had the ability to control that area had he so chosen. There are other reasons that we believe he was aware of this.

Mr. WILSON. And I am glad you have clarified that because every time I saw it on the map—even within the last 24 hours—there have been references to it, and I thought, well, you know, who does have responsibility? And so, I think it is very important to make it clear who does, and it would be Saddam Hussein.

Additionally, I noted with interest you referenced Paris, you referenced Germany and France. I know that both Germany and France have taken extraordinary efforts to go after terrorist cells and prosecute.

But are they being cooperative with our intelligence services of the United States?

Mr. BILLINGSLEA. Yes.

Mr. WILSON. Good.

And then, I share the interest of Congressman Rodriguez, too, about the civil affairs units, and I think that they are very important, and there will be additional added. And I am familiar with civil affairs units in the Army Reserves where they back up civil government. Is that what these would be largely doing?

Mr. BILLINGSLEA. Absolutely. This is one of the areas which has had some of the greatest strain because there is so much of the force structure in the reserve part of the command. So the personnel increases here are meant to not only give more capability, but to offset some of the strains that we have seen.

Mr. WILSON. I noted with interest that it was referenced about governmental areas that are non-governed, semi-governed, partly governed, maybe governed, who knows if they are governed. And so, I would think that the civil affairs units would be particularly needed when we reach those areas.

Mr. BILLINGSLEA. Depending on the ability of the host nation and their desire for that kind of help that might be a good role for them.

Mr. WILSON. I have no further questions. Thank you very much.

Mr. SAXTON. Mr. Bartlett please.

Mr. BARTLETT. Thank you.

I was looking at your unfunded requirements list. This represents the totality of your unfunded requirements or you stopped at one page?

Mr. BILLINGSLEA. Sir, I am not even sure what list you have got there.

Mr. BARTLETT. I have an fiscal year 2004 unfinanced requirements list that is in our committee handout. We will get you a copy of it. Let us know if that is, in fact, the administration's unfunded requirements list.

Mr. BILLINGSLEA. Okay. Can I ask you—the fellow who is going to follow up here is the senior acquisition executive for U.S. SOCOM and he can talk at great length about this.

Mr. BARTLETT. Okay, fine. I will ask him that question also.

I would like for the record, though, for you to look at this list and from your perspective and your responsibilities would this represent your unfunded requirements list or will you come up with a different list? And you can do that for the record.

Mr. BILLINGSLEA. Thank you, sir.

[The information referred is classified and retained in the committee files.]

Mr. BARTLETT. We would just like to know if this matches your priorities and your list or would there be a different one from your perspective.

Mr. BILLINGSLEA. Okay. We will get that to you. Yes, sir.

Mr. BARTLETT. Thank you very much.

Thank you, Mr. Chairman.

Mr. SAXTON. Mr. Larson.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

You may have already addressed this, so I apologize, but I think it is an important one to bring up.

We understand, again, the Department of Defense would like to have the authority to provide up to \$200 million of military assistance to other nations for the purpose of fighting terrorism. Can you just elaborate a little more on how you envision this authority being used?

Mr. BILLINGSLEA. There are a couple of proposals that are being made to the committee to help with giving some additional legislative flexibility. We have just found certain things as we were thrown into an unexpected kind of conflict on terrorism, and one of the things that we have found is that we are so very much reliant on coalition support, help, and, indeed, for them to conduct operations on their own or with our backstopping them that it is crucial that we be able to give them the kind of assistance they need to carry off the right kind of operations.

We need to be able to do that not only with foreign governments, but also with friendly indigenous forces, precisely as is being done right now in Iraq. And so, you will see in the administration's request to the committee for authorization two requests: One is for an ability to utilize funds for the training of, in essence, foreign governmental forces—which is, I believe, what you are talking about, sir—as well as a separate proposal from my office to be able to use funds appropriated, not to add money, but to use existing funds to train indigenous forces. And that is meant to basically bol-



ster and stand up this kind of counterterrorist capability in foreign countries.

Did that answer it?

Mr. LANGEVIN. It did. I think it is fine. I may have some follow-up questions for the record on that issue.

Next, I guess I would also like to address the fact that we know that good intelligence is key to effective use of the capabilities of our special forces. How, if you could tell me, will your office work with the newly created Under secretary of Defense for Intelligence (USDI) to provide timely and actionable intelligence to special forces?

Mr. BILLINGSLEA. The short answer is, very closely. And that relationship is already being created with the new secretary of defense. The delineation will be that USDI does intelligence and SOLIC is responsible for policy for operations. And so, that sometimes can be a fuzzy line in there, but it is a matter that we have worked pretty well in the past with the command, control, communications and intelligence (C3I), the assistant secretary for C3I in the past, so I think we will just transfer that relationship up a notch to the under secretary.

Mr. LANGEVIN. Thank you very much.

Mr. SAXTON. Thank you, Jim.

Mr. Secretary, there are a couple of recurring themes I would just like to ask you about, recurring not only here, but among people who have been dealing with terrorism longer than we have. We had—actually it was a different group—there was an Israeli here not long ago representing the Israeli Defense Forces (IDF), and he was remarking about our efforts in homeland security.

And he said something like—and he said this very nice—he said: You Americans are going to have to understand you cannot protect every target at home, that you cannot protect every government building, every bridge, every tunnel, every railroad train, every airplane, every airport, et cetera, et cetera, et cetera.

And he said: We in Israel have learned that we have got to reach out and disturb their processes, their planning, their next attacks. And not long after that, Paul McHale was here and talking about homeland security, talked about the same concept.

And I am wondering about your perspective with regard to that, and also the necessity and the process—or what I believe is a necessity and the process—of increasing or getting better intelligence in order to know where the bad guys are. Can you talk about that for just a minute and tell us what your perspective is?

Mr. BILLINGSLEA. On the first point, I think, by and large, the government of Israel has got it right. They have far fewer problems in terms of scale and scope for protection. But when you are dealing with terrorist organizations that are structured the way al Qaida and others are, playing defense alone is not an option. In fact, the best defense is probably a very aggressive offense. And so, that is the approach we are taking. There is no margin for error, especially with weapons of mass destruction looming over all of this.

In terms of intelligence, there are a number of things that can be said about that. Yes, we have to continue to pursue the kind of intelligence we need to move against these terrorist organizations.



With that said, we also as policy-makers, both in the administration and in Congress, need to recalibrate our expectations for what we assess as actionable intelligence. We need to lower that threshold to the appropriate level and we need to have a higher threshold tolerance for pain in the event that we miscalculate or things go wrong or people get caught or something happens.

Mr. SAXTON. Or noncombatants getting in the way at the wrong time.

Mr. BILLINGSLEA. All of these kinds of things, and it is a nontrivial thing in a democracy.

Mr. SAXTON. On intelligence, from your perspective, do you see the necessary changes taking place in the intelligence community? A couple of things from my perspective have happened; First, during the Cold War we had an intelligence capability that was geared to collect intelligence on the Soviet threat.

Then the—what do we call it?—the peace dividend, one of the casualties of the peace dividend was that the robust capability that was geared toward that threat was seduced. We were able to relax our intelligence-gathering capability, whether it was right or wrong, a good decision or bad decision, we did it. And now we have got a completely different set of targets to collect intelligence on, which are much different in nature than the Soviet threat was.

Have we changed? Do we need, from your point of view—have we changed enough to be able to be effective in collecting on these new targets?

Mr. BILLINGSLEA. We are in the process of evolving our capabilities. Clearly, this kind of challenge has meant that we do need to develop additional capabilities that we just did not have as tools in our tool kit. And the development of a lot of those capabilities is underway. That is something that the undersecretary of defense for intelligence is specifically charged with overseeing.

There also is a great deal of information out there. It is just knowing how to absorb it and to understand it. In fact, in some ways on the open source side you can drown in so much information. So working on ways to get that reduced down to a level where you can understand it and act on it is another big challenge for us.

Mr. SAXTON. Robin, did you want to say something?

Mr. HAYES. Mr. Chairman, if you would yield for just a moment?

You touched on something that I was trying to leave alone, but you are absolutely right. We have got a proposal from the senior senator from New York to spend \$7 billion to \$10 billion equipping civilian airlines with missile defeating systems. This is money that needs to be spent on actively pursuing terrorists through means that we have discussed here today and through other means.

So I think it makes me feel better to enter that into the record; to spend money making people feel safe is not nearly as effective spending money making people safe by catching the terrorists.

Thank you. I yield back.

Mr. SAXTON. Thank you.

Let me ask one final question.

We know that the expectations that we have and that the administration have, SOF forces have changed dramatically. We know that because we have already seen the command change from a supporting command to supported command. We know it is chang-

ing because your budget request this year is significantly higher than it was last year. We know that because you have asked for almost 2,000 additional SOF forces personnel.

There is an element in the statute which requires SOF to come to the Secretary of Defense or the President before carrying out an activity or an action and you have not requested any change in that.

And I am wondering if you might contemplate doing so or if—let me just—maybe this is just me thinking, but I conjure up in my mind, just based on activities of the last couple of weeks, when we started this war, we had—I have to be careful because I am not sure where I heard this—but we had some information that we had to act on rather quickly. And the period of time that elapsed between the time that we got that information and the time we actually took action was pretty short.

SOF has the ability to go out and plan activities and if an opportunity presents itself and you have to run back, probably through you to the secretary—through your staffer to the Secretary of Defense to get an answer on whether we should pursue this opportunity, that seems like a little bit too bureaucratic, if you will. And I do not mean to use that term in any funny way, but I am just wondering if this is a change that you are going to ask us to look at?

Mr. BILLINGSLEA. I think it probably is not a change that we are asking in terms of any statutory adjustment. With that said, we are real mindful of how in this area you need to be able to act on instantaneous opportunities or events. You do not want to get tied up in the bureaucracy. But there are a number of ways you can address that, and not all of those ways require moving up some kind of pyramid scheme. There could be conversations had at the highest level in real time.

You can also delineate at the outset, when you send folks out, what they can and cannot do and under what kind of contingencies they can execute actions using their best judgment. One of the benefits of working with U.S. Special Operations Command is the high level of maturity that the individual SOF operators have and their ability to use good judgment in those kind of situations, so you have some level of confidence in that.

Mr. SAXTON. Well, Mr. Billingslea, we thank you very much for being with us today. We have no further questions at this time. We appreciate the dedication and the effort that you put in to this endeavor. And as Mr. Wilson pointed out, we just want to do everything we can to help you do your job.

Mr. BILLINGSLEA. Thank you, sir.

Mr. SAXTON. Thank you.

Our second panel this afternoon will provide an outline of the procurement and fiscal issues facing the Special Operations Command mission. Our witness is Mr. Harry Schulte, acquisition executive, U.S. Special Operations Command. I enjoyed a great briefing with Harry some time ago at Tampa. And we are very pleased that he is here with us today. We expect that we are going to hear how the additional funds that have been requested by the administration may be utilized, as well as some other shortfalls that may exist.

Mr. Schulte.

**STATEMENT OF HARRY SCHULTE, ACQUISITION EXECUTIVE,  
UNITED STATES SPECIAL OPERATION COMMAND**

Mr. SCHULTE. Thank you, Mr. Chairman, Congressman Meehan and distinguished members of the committee, it is an honor and privilege to report to you on the topic of Special Operations Forces acquisition and technology. I will keep my opening remarks somewhat brief, but would like to submit my longer written statement for the record.

Congress through Title X, U.S. Code, Chapter 6, Section 167, empowered Special Operations Command to develop and acquire special operations peculiar equipment, material and services. We have implemented streamlined and cost-effective processes to provide our SOF soldiers, sailors and airmen with the technology and equipment they need to execute their warfighting and peacekeeping missions.

Our fundamental acquisition philosophy in SOCOM is procurement on demand (POD), in an expedited manner an 80 percent solution while working with our warfighters and industry to address the remaining 20 percent of their requirement. We leveraged the three services, the Defense Advanced Research Projects Agency, DARPA, the Department of Energy, and other agency research and development programs to look for technology to apply to our SOF warfighter needs.

We survey industry and we use a buy-and-try approach for government and commercial off-the-shelf items. Our warfighters perform early user evaluations of these potential systems then we modify them, test them, and field acceptable products to our warfighters.

We enjoy an exceptionally close working relationship with our SOF operational users. They are willing and anxious to accept the timely increase in capability provided by the 80 percent solution, and their high state of training and experience enables us to accept risk in our fielding decisions.

This process enables SOCOM to shorten the typical acquisition cycle and rapidly insert technology to provide our SOF warfighters critical war fighting advantages. The acquisition organization's collocation with headquarters SOCOM, daily contact with our warfighters, our relatively small size and short decision cycles and the support we receive from the services, the Department of Defense and Congress are major contributing factors to our effectiveness.

SOCOM's expanded role in the war on terrorism has resulted in expanded resources, as the department recognized the challenges confronting SOF and the nation. Along with the authority to budget in the program for SOF activities, SOCOM also has the authority to develop and acquire special operations peculiar equipment to prepare SOF to carry out their assigned missions.

This provides the warfighter with the tools necessary to fight not only the most committed industrial age power, but also the means to fight entities that would and could wield influence through terror by any means.

SOCOM's fiscal year 2004 procurement is about \$2 billion, more than double the amount that was appropriated in fiscal year 2003. But speaking of fiscal year 2003, we would like to thank Congress for the procurement increases received, over \$137 million, including the transfer of funds from the Defense Emergency Response Fund.

The current state of SOF capabilities is strong, but to meet the evolving capabilities of potential adversaries, we must invest now to ensure reliable support for the defense strategy.

SOCOM's aim in the pursuit and technological transformation is to guarantee our forces remain relevant to any fight and assure we minimize risk to our nation's vital interests. Highlights of the fiscal year 2004 request are included in the statement for the record.

Although our people are certainly SOF's most important asset, maintaining and improving material capabilities remains SOF's most difficult challenge. SOF must keep its equipment up-to-date while keeping the costs for sustaining its warfighting systems under control.

SOF depends on leading-edge technology to provide the critical advantage and to support participation in a growing number of technologically complex missions and operations. Our challenge is to find ways to modernize and sustain legacy systems when it makes sense, while developing technological bridges for their industry service, interagency and international partners.

On the horizon we see promising technologies maturing that will help keep SOF on the cutting-edge. SOCOM is working closely with industry, with labs, with academia, to insert those into our technology-thrust areas.

Our thrust areas are signature reduction, high bandwidth reach-back communications, underwater communications, unmanned systems, batteries and fuel cells, remote sensing, advanced training systems, bio-engineering and directed energy weapons. These thrust areas address the technology gaps we see and offer SOCOM the greatest opportunity for technological payoff.

SOCOM's fiscal year 2004 research, development, test and evaluation (RDT&E) request is \$440.4 million as compared to \$512.5 million in fiscal year 2003, which included net target at congressional plus-ups of about \$92 million.

In conclusion, SOCOM has worked hard to wisely use its modernization resources to sustain systems where it makes sense, to integrate new technologies into legacy systems and to acquire new technically advanced systems. We intend to continue our focus on modernization and transformation challenges to ensure our ability to rapidly adapt to changes in technology, the operational environment, and to assure we always provide our SOF operators with the decisive advantage.

Now and in the future, SOF continues to improve their ability to execute the war on terrorism while remaining ready to deal equally with demands of both our warfighting and peacekeeping roles.

Thank you for your interest in and continued support of our soldiers, sailors, airmen, Marines and civilians, the men and women of the United States Special Operations Command.

Mr. Chairman, I am open for any kind of questions.

[The prepared statement of Mr. Schulte can be found in the Appendix on page 348.]



Mr. SAXTON. Thank you very much.

Mr. Meehan.

Mr. MEEHAN. Thank you, Mr. Chairman.

Mr. Schulte, the SOCOM aircraft modernization budget relies heavily upon the development and fielding of the CV-22, the Special Operations variant of the Marines Osprey. If the Marine Corps were to cancel this program for any reason, is there an alternative recapitalization plan for SOCOM?

Mr. SCHULTE. There is probably not a plan at this point in time, although we have looked at what would happen if for any reasons the program went away, whether Marines would cancel or what. The interim solution would be we would have to do a service of life extension program on our MH-53 fleet, of which we have about 38 MH-53s at Air Force Special Operations Command.

Right now we are planning on taking the MH-53s out of the inventory between fiscal year 2009 and fiscal year 2014, I believe it is. So if we were going to have to keep them any longer, we would have to institute a service of life extension program. Then we would have to go back and probably re-look at a new program to satisfy the need that the CV-22 would have fulfilled. We have an operational need for aircraft to do the kinds of things that a CV-22 can do. If we are not going to have the CV-22, the requirement does not change. We have still got missions today that we cannot do with our current fleet. And so, if that went away, we would have to start over again and see what other kind of new technology you could bring, and that would be a long process.

Mr. MEEHAN. Given the importance of SOCOM, would it be a good idea to maybe look and have your own plan in the event that the Marines were to cancel the program?

Mr. SCHULTE. Let me put it this way, we are really embedded well with the Marines on the V-22 program, and right now I think both the Marines and SOCOM are cautiously optimistic that the program is looking good. Over the next two years, we are going to know a lot more. I think you are exactly right, if this thing does not prove out in the next couple of years, we are going to have to go back and do something. In the meantime, we can do an interim solution with the MH-53s, but we are going to have to go back to the drawing board.

But right now I think—you know, the test program just got re-started last year. I think the Marines started flying in May of last year. We started flying in September of last year. There have been about 300 flight test hours total between the fleets. So far things are looking good. It has been a crawl, walk, run to get the program back up to where we would like it to be. But the data is looking good, and we are optimistic; not to say that something could not happen that is unfortunate, but right now it is looking good.

I think one of the concerns on Mr. Aldridge's part has always been the high rate of descent testing. Well, I think we are going to know about that probably by June of this year. Most of that testing will be done. That was a real concern up front. I think so far all of that data is looking good. There has been a lot of testing done on that by the Marine Corps. I think that issue may end up going away, and we will know that for sure in a few months.



For our side of it on a CV-22, our concerns are associated with the extra equipment that we have added to the aircraft, like the terrain following trainable and radar. We have got a directed infrared counter-measure system on the aircraft. We have got radio frequency (RF) counter-measures and different kinds of electronic warfare. This is what we need. We need to prove out on our side.

The Marines will prove that the airplane works; we have got to prove that the additional systems that we are putting on it that do the kind of missions that SOF needs to do is going to work. We are going to know that later than the Marines are going to know. The Marines will know a lot this year, and really it will be in great shape by next year.

Mr. BILLINGSLEA. We will know quite a bit, maybe, a year from now. And I think, you know, if things go the way they are going right now, it is going to look real good. If by then, you know, it is looking bad, you are exactly right, we are going to do something.

Mr. MEEHAN. You can make an adjustment and come up with a plan.

Mr. BILLINGSLEA. Yes, sir.

Mr. MEEHAN. Thanks very much.

Mr. SAXTON. Thank you.

Mr. Lobiondo.

Mr. LOBIONDO. Thank you, Mr. Chairman.

With an increase in your SOCOM budget for 2004, how will this influence the procurement of CV-22s?

Mr. SCHULTE. A small portion of that \$1 billion increase in procurement is for CV-22. Basically, we are buying two aircraft; two CV-22 in 2004 and it also includes the advanced procurement money for three aircraft in 2005. So there are about \$50 million in that additional \$1 billion of procurement for CV-22; two aircraft in 2004 and the advance buy for three aircraft in 2005. So the buy profile right now for CV-22 starting in 2004, is \$233,255, I believe it is.

We recognize, and I think the department recognizes, if this testing turns out well, and again, we are hopeful that it will, that it is probably too slow to buy the aircraft, quite frankly. But it is too early to try to accelerate anything. We just do not know enough.

So in a year, year and a half, if everything is working out okay, I think you might see SOCOM come back to the department and, in turn, may come back to Congress and say, "Buying these things in two and three and even five a year"—by the way, that takes us to the year fiscal year 17 to get our 50 aircraft.

If this thing works out and everybody agrees over the next couple of years, you are going to see SOCOM come back and say, "We need to buy those at a quicker pace than that so that we are not out 14 years to get 50 airplanes." It is not a particular economic rate for us either. But for fiscal year 2004 there are about \$50 million additional for the procurement of CV-22s.

Mr. LOBIONDO. Thank you.

I know I probably speak for all of my colleagues that we are concerned about the number of deaths from helicopter accidents recently, especially in comparison to those killed in direct combat with the enemy, and we certainly do not ever want to put our troops in a situation where their equipment is not up to snuff or

causing a problem. But the average age of your helicopters—I mean it has to be pretty much up there?

Mr. SCHULTE. The average age of the Air Force aircraft, in general, including the MH-53 helicopter, averages 32 years.

The average age of the Army rotary wing fleet is about 14 years; 14 years, and those aircraft, as you will see in the budget request, are going to be going through a service life extension program. So they kind of get zero timed out and get started over again. But clearly, the Air Force fleet is aging and has significant age on it now.

Mr. LOBIONDO. Well, I certainly would like to join with our chairman and probably the full committee in helping you with your rotocraft problems. It seems to me that this is something that we have got to aggressively address in light of what has happened recently.

Mr. Schulte, thank you very much.

Thank you, Mr. Chairman.

Mr. SAXTON. Thank you.

I guess I would just like to share with everybody an experience that I had back when I came to Congress in 1985. The C-17 was a design on paper, and we took something like 13 years to develop what I now believe is a revolutionary way to move people and equipment. And the V-22 is, in my view, equally revolutionary and presents an equally difficult, time-consuming set of problems. And I am very optimistic that given the progress that I have seen on the V-22, that we are going to be okay, and we almost have to be.

Mr. SCHULTE. Yes, sir.

Mr. SAXTON. Mr. Kline.

Mr. KLINE. Thank you, Mr. Chairman.

Very briefly, you talked about the SOCOM's procurement profile for the CV-22. How does that meld with the Marines' MV-22?

Mr. SCHULTE. The Marines' profile, as you know, sir, is quite a bit higher, but it is all part of the program. Right now we are limited to a minimum sustaining rate of 11 aircraft per year until we get through some of these problems—

Mr. KLINE. Between the two?

Mr. SCHULTE. Between the two of us. We are working very well together on staying at that 11. I think there may be a decision later this year that says, "Okay, I think you can maybe go up to 15 or something like that." We are hoping that would happen, and then it would give room for both of us to increase the rate.

Mr. KLINE. Okay. Thank you.

I yield back, Mr. Chairman.

Mr. SAXTON. Thank you very much.

Mr. WILSON. Again, with the unfunded or unfinanced requirements that you have indicated, with the higher budget that you have, are there any items that there should be a special effort made by people that you would like made?

Mr. SCHULTE. Well, our first priority, of course, is the budget that the president submitted. The items that you see on the unfunded list—and I have got a copy of it in front of me, too—are the next priority items that the command would like to buy, and if we had not been resource constrained—albeit we got a lot more money this year so we are not complaining—but were there even more room, we would have picked off some more of these items; some of

these items like the advanced light-weight grenade launcher, which is our number one unfunded requirement.

We are buying some of those items in the fiscal year 2004, but this actually buys it out. This buys all we are going to need, including the ammo, and it gets it out to everybody right away, and you will see that in a number of cases. The number two unfunded is the Riverine craft. That is for 10 of those, and that buys that out.

We will have delivered ten through the end of this year. This buys the other ten, and that is the full complement that we are looking for. These are funded in the out years, the other ten, but if we could, you know, pull them forward, that is what this means.

But this is a priority. This has been through the Army component, the Navy component, the Air Force component. This has been looked at by General Holland, and this is his list—this is the priority of the things that the command needs that we were not able to get into the fiscal year 2004 budget.

Mr. WILSON. It looks like a very reasonable list to me and not a wish list but one that would assist you in achieving the extraordinary goals that you have.

Mr. SCHULTE. Yes, sir. I think so.

Mr. WILSON. And I certainly would want to join with the chairman to assist.

Mr. SCHULTE. Thank you, sir.

Mr. WILSON. Thank you.

I yield the balance of my time.

Mr. SAXTON. Thank you.

Mr. Akin.

Mr. AKIN. Thank you, Mr. Chairman.

Just a quick question. It is sort of a piggyback on Mr. LoBiondo. The helicopter accidents we have seen, is there a pretty good indication that those are a result of the age of the aircraft or are those a result of other things? Do you have any kind of numbers on that?

Mr. SCHULTE. Sir, I really do not. But they are kind of all over the place. You know, we had 11 helicopters damaged in Operation Enduring Freedom. Two were completely destroyed. These were MH-47s, by the way. But two were completely destroyed. You may remember the one up on the ridge, Anaconda, and the other one we lost in the Philippines. That was an accident in the Philippines.

There was no indication that that was age-related or anything like that and, of course, up on Anaconda people were shooting at those guys, so that is what took that helicopter out. And most of the other ones that were damaged were damaged due to fire.

They were in combat and they were hit. Now, the other nine of those 11 we were able to bring back and fix, and it takes about six months on average to get those fixed and get them back into the fleet. That is what we have been trying to do.

I do not really have data that says, "Hey, these things are failing or are crashing because they are old." Some of them are old. The Army helicopters are not as old as the Air Force helicopters, but they are very well maintained. So I do not think you are seeing accidents necessarily due to age. You know, you are seeing accidents in combat.

Mr. AKIN. Some of them because people drilling little holes in them.

Mr. SCHULTE. Yes, sir. That is true.

Mr. SAXTON. I think Mr. Hayes may have a question.

Mr. HAYES. Thank you, Mr. Chairman.

I just wanted to comment. Mr. Meehan and I were having a discussion about the validity and the value of his question. I have not found in my research anything out there that fills the gap between where we are in the V-22.

So what I would like to recommend to you and to our committee is that sufficient funds be provided so that we could put more platforms into a more robust testing program, not to compromise safety in any way, but to make sure that we are doing the things simultaneously we can to bring that platform on line or to say this is not going to work. So I would like to enter that into the discussion.

And thank Mr. Meehan for his question.

Mr. SCHULTE. Well, thank you, sir. And I was probably remiss in not bringing up that one of the things we are trying to do—the department asked us back in the fall, you know, take a look at accelerating the CV-22 program, and we did take a look at that. Quite frankly, General Holland felt and the Marine Corps agreed, that that is sending the wrong signal right now. There will be the right time to address accelerating the CV-22 program, but maybe it is a year from now or something.

But the one thing that did come out of that study, and the one idea that everyone agreed with was, we need one additional test aircraft. And so, what we have done is tried to find the money from within the command to the extent that we can.

There is money in the 2004 bill that is over in the Navy line that was going to be used to operate this third test aircraft for the CV, if we got it built in time. It turns out that we were not able to get it done that quick. And so, that money is available to help us modify that third test aircraft.

So we found some 2002 money—this is R&D money—we found some 2002 money. We are going to be asking you to reprogram a little 2003 money when our reprogramming bill comes over.

And there is a little bit of 2004 money, \$29 million, that is in a Navy line that needs to go into a SOCOM line. The Navy agrees with this, by the way. This is not hostile takeover or anything. That would give us \$66 million that would allow us to take a Marine MV-22 and modify it into a CV test aircraft; that would give us three test aircraft.

Now what that really does, it accelerates the test program a little bit, but not very much by the time we got to do it. But what it does, it makes it much more robust. If one of these test aircraft—we have only got two—if you have three and one goes down, you still have two. You got two and one goes down, you got one; now you are in real trouble.

Mr. HAYES. The point you are making is very important. There is no compromising of safety. It is not acceleration. It is just providing more assets to do the program more safely—

Mr. SCHULTE. It will allow us to get through the test program better.

Mr. HAYES. Thank you.

Mr. SAXTON. We are going to try to finish up before these votes so we do not have to keep you waiting around here.



Let me just ask you a question. I looked at your list—and this is just a curiosity item. I had the wonderful opportunity to fire some weapons out in the desert of California with the SEALs. And I laid down there and I started pulling the trigger on the M-4 and she jammed up on me.

Mr. SCHULTE. Yes, sir.

Mr. SAXTON. I asked some questions about that, and I learned that that is maybe not as infrequent as we would hope with that weapon, and I do not see it as a priority item here, and I am curious to know, maybe, why that is.

Mr. SCHULTE. We have done a fair amount of trying to enhance reliability of the M-4. We put an extraction enhancement kit together that both the Army and the Navy guys that use the M-4 have.

We put heavy barrels on the weapon for the Army. We put a new upper receiver group on the weapon for the Army. We are designing a new magazine for the Navy version of it that will be more reliable. And in fact, for the guys, NSW Crane is going to rebuild the weapons every 12 to 18 months. So we are doing everything we can do for the M-4, I think.

What you will see in the 2004, in the budget is, there is some R&D money beginning in fiscal year 2004 for a special operations combat rifle. This would be a follow-on to an M-4. There is a small amount of R&D money in 2004, again in 2005, and then some production money in 2006 and out. But we are going to work very closely with Army program manager for soldier weapons up at Picatinny Arsenal. They have got an individual combat weapon and an objective cruise—

Mr. SAXTON. Is it a heavier caliber?

Mr. SCHULTE. It might be a heavier caliber; that has not been decided yet. We are still working with the joint operational requirements doctrine throughout our command. It could be a heavier weapon; that has not been determined yet.

Mr. SAXTON. One of the things that I learn by asking a lot of questions is that, sometimes it takes multiple hits to take a guy down with the M-4, and that seems like maybe something we should look at fixing.

Mr. SCHULTE. One of the things we did in the short-term is we heard that—you know, we have got some reports back from Afghanistan that sometimes it was tough taking these guys down with the M-4. What we did do was go out and test the 77 grain bullet, and, by the way, that tested out very well. The problem that you have with the M-4 and the bullet that is in it right now is it does not tumble.

And so, if you are at relatively close range, let's say, you know, 30 or 40 meters on this thing, it will have a tendency to go right through someone because it is not tumbling. And if it does not happen to hit a vital organ, and sometimes it does not, then that guy keeps going, at least for a little while, and our guys really hate that. So if you go to the 77 grain, the test, as this thing will start coming—

Mr. SAXTON. Especially if they are coming this way.

Mr. SCHULTE. If they are going the other way, that is not—and so, we have done the testing on this 77 grain. It is still a 556



round, but it is a little heavier 556 round. It tends to tumble a little sooner. Tumbling means when it hits it causes a lot more damage.

Mr. SAXTON. Mr. Cooper has a question.

I wanted to ask you about the Advanced SEAL Delivery System program, GAO just issued a report on it. But I will put it in writing and send it to you.

We will go to Mr. Cooper.

Mr. COOPER. Just a small quick question about a small, but important item, battery power. How dependent are special forces on these little pesky things? And are you working with DARPA to try to improve the technology?

Mr. SCHULTE. We are working with anybody and everybody on batteries. We worry about batteries for the advanced SEAL delivery system. We worry about batteries for the soldier in his backpack. We are working with everybody we can think of, including DARPA, the CIA and other folks that are working on batteries, and we have got our folks plugged into everybody that is doing anything on it.

You know, we need to get them to last longer. We need them to be lighter. We are looking at rechargeable kinds of batteries and things like that. You know, it is a big item. I mentioned it in one of our thrust areas in our technology. We are talking to anybody and everybody that is got ideas on batteries. It is really important to us.

Mr. SAXTON. Okay. Thank you very much, Mr. Cooper.

Mr. Schulte, thank you very much.

We have got about five minutes left before we have to push the bottom over there, so we are going to run.

Mr. SCHULTE. Okay. Thank you very much.

Mr. SAXTON. Thank you very much. It has been a great hearing. And we look forward to working with you.

Mr. SCHULTE. Thank you, sir.

[Whereupon, at 3:33 p.m., the subcommittee was adjourned.]



---

---

# **A P P E N D I X**

APRIL 1, 2003

---

---



---

---

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

APRIL 1, 2003

---

---





**Statement of Chairman Jim Saxton  
Subcommittee on Terrorism, Unconventional Threats and  
Capabilities**

---

**Subcommittee Hearing on Special Operations Command Budget  
Request for Fiscal Year 2004**

---

**April 1, 2003**

**Chairman:** Gavel down. Brings meeting to order.

[Makes the following statement.]

The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this afternoon to consider the fiscal year 2004 budget request of the U. S. Special Operations Command. This will be an unusual hearing in several respects. No combatant command with the exception of Central Command is more engaged in Operations Iraqi Freedom and Operation Enduring Freedom than the U. S. Special Operations Command. SOCOM units are in combat, and SOCOM units will be needed to participate in the rebuilding of Iraq, and they are participating in the rebuilding of Afghanistan. Unlike Central

Command, which has forces provided by the services as needed, SOCOM relies continuously upon the same group of 46,000 troops that are a permanent part of the command. They are indeed intrepid warriors, and I am proud that they are American fighting men.

Because the command is at war, we have excused the commander and deputy commander from appearing before the subcommittee. However, since we are moving forward with our markup in early May, and since the fiscal year 2004 budget request for SOCOM reflects substantial increases in personnel, mission, and funding, we must, as the oversight subcommittee, hold a public hearing on SOCOM's part of the budget request.

My colleagues know of my regard for special forces troops. I have visited all elements of special forces in recent months and have been uniformly impressed with the professionalism and patriotism found throughout special forces units. The results of their efforts speak for themselves—special forces have been brilliantly successful in Afghanistan and Iraq—they are our nation's best weapon in the Global War on Terrorism.

The subcommittee understands that necessary wartime costs will be funded in the supplemental appropriation request now working its

way through Congress. Nevertheless, the budget request represents a large peacetime, enduring commitment to a great number of special forces and resources. It is important for the subcommittee to receive testimony on these issues in open session.

While I believe that SOCOM units are our best weapon in the war on terrorism, I also worry that SOCOM units may be overused. I have heard repeatedly from senior commanders and understand from my personal observations of these fine men, that special forces operators cannot be mass produced. Members have also heard of problems with aging and overused equipment, particularly aviation assets. As a small, highly specialized, and highly trained elite force, there are never very many special forces of any kind. Against that backdrop, and the temptation to overuse this force, I wonder what the long term plan is, and look forward to hearing testimony on that point.

SOCOM, unique among the combatant commands, has a statutory mission list and special statutory procurement authority. The subcommittee will ask whether the mission list should be adjusted given the rightful emphasis on the counter-terrorism role, to find some other means to accomplish missions of lower priority. I am confident that SOCOM enjoys the special procurement authority, and the subcommittee will inquire on how it is being used.

Our first witness, Mr. Marshall Billingslea, is the senior policy making office in the Department of Defense for special operations related matters. As such, he speaks for the command within the Pentagon and advises the Secretary of Defense on special operations budgets, roles and missions.

**Chairman:** Yields to Mr. Meehan for any opening remarks he may wish to make.

**Mr. Meehan:** Makes opening remarks.



Testimony Before the House Armed Services Committee  
Subcommittee on Unconventional Threats

By  
Marshall Billingslea  
Principal Deputy Assistant Secretary of Defense  
Special Operations / Low-Intensity Conflict

April 1, 2003

MR. CHAIRMAN, Congressman Meehan, members of the subcommittee, I appreciate your invitation to testify before the committee to update you on the progress we are making in prosecuting the war on terrorism, and to describe for you the strategy we are implementing today, along with the significant implications that strategy has for the United States Special Operations Command (USSOCOM) and Special Operations Forces (SOF).

I do ask your indulgence today. As we are in open session, and I am not well-equipped to answer any specific questions regarding Iraq, I am going to stay away from any issues that might have bearing on ongoing operations (although I will try to provide a little context regarding the role of Special Operations Forces in that conflict).

*The Bottom Line*

I will give you the bottom line at the outset. The United States and its allies have made significant progress in destroying and disrupting key parts of the international terrorist network with which we are at war. Al'Qaida is an organization under great stress, with a leadership that seems increasingly less able to plan multiple large scale attacks because they are focused on the more immediate problem of evading coalition capture.

USSOCOM has been a key player in that effort, and is working hand-in-glove with other parts of the U.S. government and with coalition partners. The President's FY04 budget initiates a significant transformation of USSOCOM into a supported combatant command for the war on terrorism, and alleviates a number of the mounting problems incurred by such a high OPTEMPO for the Command.

However, having given you this assessment of al'Qaida, I hasten to add a key qualifier: we are certain that we do not know all of the planning that al'Qaida has already done, and we are concerned that they may have set certain operations in motion before the most recent chain of events leading to Khalid Shaikh Muhammad's capture. Moreover, al'Qaida and affiliated terrorist organizations have proven capable of regenerating lost parts, and of changing tactics and techniques to adapt to our offensive efforts.

To put it simply: Al'Qaida and other related terrorist groups today remain intent on conducting devastating attacks against the United States, our friends and allies. At least some of their planning seems to contemplate the use of chemical or biological agents. But as the October 2002 attack using an explosives-laden dhow against the French oil tanker in Yemen showed, low-tech, conventional explosives continue to afford terrorists the ability to mount attacks with devastating consequences.

### *The Nature of the Enemy*

Before I describe for you specific progress that we have made to date, I first need to explain to the Committee how we perceive the international terrorist network. Once I have sketched that out for you, you will be able to see how we are targeting key strands of this network.

Al'Qaida is perhaps best viewed as part of a spider web. At the center of the web are a number of terrorist groups – dozens actually, of varying sizes with varying agendas. Al'Qaida and its proxy groups, such as the IMU in Uzbekistan, and Jemaah Islamiyah in Indonesia, and Abu Sayyaf in the Philippines, and EIJ in Egypt, and various Algerian, Chechen and other radical groups. From this core of the network spread tendrils around the globe. They reach deep into those rogue states that the Counter-Terrorism Coordinator and the Secretary of State have labelled as “state-sponsors of terrorism” (i.e., Iran, Iraq, Libya, Syria, Sudan, Cuba, and North Korea). The web reaches deeply into the ungoverned and less-governed zones of the earth, the triborder area in Latin America, parts of Yemen and Pakistan and Afghanistan, certain of the islands of the Philippines and Indonesia, parts of Lebanon, Somalia, and other parts of Africa.

The web attaches itself to thousands of points, reaching into foreign educational systems – the madrassas. It is woven throughout religious institutions, where terrorists posing as religious scholars use their mosques to spot and recruit suicide bombers, or generally use the pulpit to spread hatred and venom against the United States. It has spread into non-governmental organizations, and charities, that are used as Trojan Horses to move people and finances around the world. The tendrils creep into certain banks and the hawallah system, and into various media outlets. The tendrils are also interwoven with other transnational “webs.” There are linkages to weapons smuggling, and drug running rings, and to proliferation networks.

The web, frustratingly and worrisomely, reaches well into friendly nations. Nearly every NATO partner has uncovered one or more al'Qaida cells. In fact, the terrorist network reaches right into our own backyard, into America. As the President mentioned in the State of the Union address, Buffalo is but one city that we have discovered to be penetrated by the al'Qaida network.

As you can see, this is a very different type of enemy that threatens the American people today. The adversaries of the Cold War – generally speaking – had a statist structure with centralized command and control, and a leadership structure which could be targeted frontally, and linearly. This network has none of those characteristics.

The spiderweb of loosely-organized terror groups has no single, integrated command structure. While the leadership of some key organizations can be eliminated, those organizations do not necessarily cease functioning. We have seen cells either continue to operate quasi-independently, or begin to coordinate with other terrorist organizations. Specific terrorist organizations themselves have flexible lines of control that – in some cases – make senior operational coordinators interchangeable with various cells. By that I mean that they can supplant one another in event of capture, and persist in execution of operations. Likewise, these organizations are capable of replacing lost leadership by nominating operatives and elevating them in stature. Obviously, key arrests can, and do, disrupt terrorist attacks. But some of the groups in the international network (and al'Qaida in particular) have proven themselves exceptionally patient and deliberate. We have seen instances where the planning for an attack was temporarily suspended after an arrest or death, only to resume a few months later with new personnel leading the charge.

### *Bringing to Bear All Elements of National Power*

Clearly, when faced with such an adaptive organization, we cannot apply pressure sporadically or unevenly. It has been necessary for us to engage, quite literally, in a “full court press,” bringing to bear all elements of our national power. Striking at this network has necessitated an unprecedented level of cooperation among U.S. defense, intelligence, law enforcement, and diplomatic agencies. There has been much commentary by those who have followed U.S. counter-terror efforts over the years regarding the transformation that has happened within the United States government, and over the strong unity of purpose that we all have in prosecuting the global war on terrorism. Likewise, the galvanizing effects of the September 11<sup>th</sup> attacks, and the subsequent Bali bombings and other events, have given rise to an unparalleled level of cooperation on a global scale between the departments and agencies of numerous foreign governments, acting both in concert with the United States, with one another, and on their own.

There is truly a global coalition against terrorism. That coalition has had some stunning successes. I must say at the outset that diplomacy has proven an essential tool in the war on terrorism, not only in maintaining coalition cohesion, but in facilitating the direct apprehension of key individuals. Our colleagues at the Department of State, within Ambassador Cofer Black's office, and at embassies around the world, are on the front line in the war on terrorism. In our estimation, within the Department of Defense, they are doing a superb job. In particular, I commend to members of the Committee, and to your staff the recent testimony given by Ambassador Black before the House International Relations Committee. His testimony provides the diplomatic context to the Defense Department assessment I am providing you this afternoon.

### *Denial of Sanctuary*

As I noted in my description of the terrorist network, the groups that are today conspiring to commit mass murder of American and allied citizens operate overtly out of

a handful of terrorist sanctuaries. The United States government is systematically draining those swamps in a denial of sanctuary campaign. Afghanistan was the first such territory, post-September 11, that the United States liberated from the grasp of terrorist organizations. In losing Afghanistan, al'Qaida lost its ability to continue using the enormous, two-decades-old infrastructure of paramilitary training camps scattered throughout the country.

Those camps, begun as a largely secular, ad hoc indigenous reaction to the Soviet invasion of Afghanistan in 1979, morphed over the ensuing decades into a hodge-podge of Islamic-fundamentalist facilities churning out a network of Arab *mujahideen* who earned their spurs in the Afghan-Soviet conflict and then returned to their homes to foment *wahhabist* insurrection in their native lands. The more extremist elements of that mujahideen network can be found scattered throughout the international terrorist network, though obviously some mujahideen did not ever, and do not today, subscribe to the wild fanaticism of a Bin Laden, or to his terrorist tactics.

The loss of those camps had an immediate and obvious impact on al'Qaida. Gone were the training facilities, and the chemical and biological research laboratories they had created, along with some of the equipment they had procured. The leadership now is scattered, and trustworthy communications are much harder to have. But the loss of Afghanistan has had a deeper, intangible effect on terrorist organizations that is hard to describe. There no longer is an equivalent place where aspiring young terrorists can go to demonstrate their commitment to fundamentalist extremism, and to receive a rigorous physical and operational regimen. The camps of Afghanistan had a deep, unifying psychological effect on the international terrorist network, as operatives trained in the same camp claim a bond of "kinship" and unity of purpose that cannot be easily replicated when those camps have been destroyed.

Of course, al'Qaida and other terrorist groups continue to find sanctuary in other countries, and are seeking to set up new camps. Iraq is one such place. We are now in the process of denying al'Qaida and other terrorist groups sanctuary there. At a very early phase of the campaign in Iraq, the United States struck multiple terrorist training facilities and encampments in Iraq. The facilities, run by an extremist Kurdish organization called Ansar al'Islam, had become over the past year and a half, safe-haven to several al'Qaida operatives and home to part of al'Qaida's chemical warfare program. In the months prior to *Operation Iraqi Freedom*, the Ansar camps had grown with foreign fighters seeking an opportunity to conduct terror attacks against the United States. It is difficult to say, at this stage, how much damage has been inflicted on Ansar al'Islam and al'Qaida. In total, we believe there to be more than a dozen terrorist groups operating from sanctuaries in Iraq. Our goal is to eradicate their presence from this country.

Finally, al'Qaida and other key terrorist organizations operate in the ungoverned areas of the earth, in between the seams of civilizations and governance. And we are striking at those terrorist concentrations when and where we find them.

### *Degrading Terrorist Finances*

Denial of sanctuary is but one aspect of the campaign. Degrading terrorist finances also is crucial. Degradation of finances translates into a degradation in operational capability. For instance, without funds, terrorists cannot move around as easily or as quickly. Weaponry on the black and grey markets, especially explosives, still takes a fair amount of cash, and there are always living expenses and other costs that have to be defrayed. The Secretary of State, working with the Departments of Treasury and Defense, and with the law enforcement and intelligence communities, has taken steps to freeze the assets of, block travel by, and criminalize relationships with, 36 different foreign terrorist organizations. Sixty entities have been listed under Executive Order 13224, and 48 groups have been designated pursuant to the USA PATRIOT Act. These legal tools, taken in conjunction with a number of international legal instruments, provide a critical basis for working with the global financial community to block assets, and to expose and dismantle terrorist-run or terrorist-penetrated non-governmental organizations, charities, and banks.

That said, it does take a great deal of money to conduct terrorist operations. Tens of thousands of dollars, not even hundreds of thousands, are often all it takes to spin up a cell to commence operational planning. That is why the freezing of more than \$100 million in terrorist finances is so significant. Equally important, we have been able to identify several key terrorist financiers, and take steps against them. The al'Qaida financier, Hawsawi, has been captured, as have some key couriers and al'Qaida "bag men." Further, some parts of al'Qaida's Southeast Asian network of front companies, NGOs, and bank accounts have been rolled up. The United States continues to track the activities of other key financiers in the Middle East, and are pressing key coalition members to take greater steps to curtail their activities.

### *Disrupting Terrorist Leadership*

The United States and coalition partners also have made progress in systematically reducing terrorist rank and file, and in capturing or killing terrorist leadership and senior operational planners. Since September, 2001, more than 55 terrorist leaders and planners have been captured or killed. In the past six months alone, there have been more than 30 arrests and seizures in 20 different countries, not counting ongoing U.S. military operations in various countries.

Two prominent al'Qaida, Muhammad Atef and Abu Ali al-Harithi, have been killed. Several other prominent operatives, such as al-Nashri, Abu Zubayda, Ramzi bin al'Shibh, al-Libi, and al-Jazairi are in custody. And, of course, the terrorist we believe was the mastermind of the September 11 attacks, Khalid Shaikh Muhammad, is now under coalition control.

I suspect, that with Khalid Shaikh Muhammad's arrest, Bin Laden and other key members of al'Qaida sleep less easily at night. Khalid's arrest is only the latest in a string, following on the January arrests by Spanish authorities of more than a dozen



terrorists along with a significant weapons cache; and the February arrests in Italy of more than two dozen al'Qaida "sleepers." His arrest was, in turn, followed by the March 2003 captures of al'Qaida operatives reported in Kenya. When you add to this the previous progress made in destroying part of the al'Qaida "Poisons Network" through arrests in London, Paris, and Spain, and some of the progress that has been made in the United States (with arrests in several cities) you see an organization that surely must be feeling the effects of our combined efforts.

Jemaah Islamiyah – a terror group closely tied to al'Qaida -- also is under strain. There has been an unprecedented level of cooperation between the nations of Southeast Asia in destroying this network. In the past 6 months, Singapore has rolled up at least 21 JI members; Indonesia has arrested the senior JI spiritual leader, Abu Bakar Bashir, the JI Operations Chief (Mukhlis) and a senior member (Kasteri); there have been other key arrests in Malaysia, Thailand, and the Philippines, although a key JI figure – Hambali – is still on the run.

I could go on at length through the other groups that comprise the international terrorist network. Abu Sayyaf which has several links to al'Qaida, has suffered some key losses. But though the Armed Forces of the Philippines has mounted a major operation on Jolo Island, ASG continues to pose a significant threat in the Philippines, and we are seeing renewed violence from the Moro Islamic Liberation Front (MILF) and the Communist Party's insurgency – the New People's Army. Similarly, notwithstanding some significant successes by the Uribe Government in Colombia, the FARC and ELN continue to pose a threat to U.S. citizens, and are holding 3 DoD government contractors hostage, having already executed one. We also continue to take efforts against the IMU in Tajikistan, and Uzbekistan, Hekmatyar and his group in Afghanistan, and numerous other organizations.

### *Destroying Terrorist Cells*

With respect to "terrorist cadre" – the footsoldiers and cell members – more than 3000 operatives have been captured in over 100 countries by the international coalition. The United States itself today detains at Guantanamo Bay nearly 700 enemy combatants including operatives and mid-level planners encountered on the battlefield. These enemy combatants are being questioned for information they hold regarding planned future terrorist attacks. The information they are providing has enabled us to better understand the nature of the global terrorist network – how key organizations operate, build cells, move money and people, and recruit individuals – and thus how to dismantle these groups. Based on their information, and that extracted from other sources under foreign control, the U.S. has been able to disrupt, or cause to fail, more than a score of planned attacks.

### *Disrupted Attacks*

Failed and/or disrupted terrorist attacks have run the gamut in terms of target and venue, and scope, ranging from the "dirty bomb" (radiological dispersion device) plan

against the United States, to plots in Italy, London, France, Germany, Colombia, Israel, Singapore, Morocco, Russia, Indonesia, the Philippines, Spain, and Turkey - to name only a few.

As an aside, it also is important for the Committee to know that the United States, working with a number of key coalition partners, has been able to disrupt and avert a string of terrorist activities being orchestrated by the Iraqi Intelligence Service using terror groups as proxies. For instance, in the Philippines, the Abu Sayyaf Group publicly announced the financial support it was getting from Iraq to conduct terror attacks against U.S. nationals. You may have noticed the large number of Iraqi operatives being evicted or arrested worldwide. We do not know the extent to which we have stopped Saddam's operatives from mounting terror attacks, but we certainly have thwarted some of their plans.

### *Ongoing Threat of Terrorism*

That said, the United States and its coalition partners have not been able to prevent key terror attacks. Jeemah Islamiyah's bombing of the Bali resort killed more than 200 innocents, including 7 Americans. Despite several seizures of car bombs by Colombian authorities, the FARC recently executed a bombing against a club in Bogota, which killed 34 and wounded 150. Similarly, the bombing of the Synagogue in Tunisia, and the attacks on the hotel in Kenya and the *El Al* flight, are examples of operations that we were not able to avert. Moreover, some groups have adjusted their planning to account for our efforts, and have "gone small-scale and local". The assassination of Lawrence Foley, a US AID employee, is an example; although the Jordanian government recently did catch two of the terrorists involved in that attack, I am pleased to report. Other examples include the bombings launched by Abu Sayyaf in the Philippines, and the targeting of U.S. Marines by terrorists operating in Kuwait. And, as I said at the outset, we know that al'Qaida and other groups continue operational planning for significant terror attacks, and may have some plans nearing the execution stage.

That brings me to an important point. The war on terror has come at great cost to the American people, and our losses on September 11<sup>th</sup> were not the last of it. Since that time, a number of American patriots have given their lives in service of the nation. Several U.S. departments and agencies have lost people; I mentioned Lawrence Foley. The Special Operations Community, in particular, has lost several of its best and brightest: to date, there have been 137 SOF wounded, 91 of whom sustained injuries during combat. Thirty eight SOF have been killed in the course Operation Enduring Freedom and related counter-terror operations.

### *The Role of Special Operations Forces (SOF)*

For the Department of Defense, U.S. Special Operations Forces are at the "tip of the spear" in waging the war against terrorism. One of the first blows struck in the war against terrorists was the fight to topple the Taliban and deny al'Qaida sanctuary in Afghanistan. That effort was waged, on the ground, by less than 500 Special Forces

personnel. They mounted an unconventional warfare effort, tied closely to indigenous forces and linked with the United States Air Force, in a way that provided for a rapid, decisive, and crushing defeat of the Taliban's conventional forces. The operation in Afghanistan was prosecuted by small units that operated with autonomy in a highly fluid environment. It was won by people who could meld with friendly Afghan forces, who could and would:

- operate without a safety net;
- develop such a rapport that they could trust their security to their Afghan allies;
- live without a huge logistics train to provide equipment and supplies;
- be able to distinguish between combatants and non-combatants in an environment where civilians and fighters, Taliban and non-Taliban, and ex-Taliban, were all jumbled together; and
- able to engineer combined arms operations between U.S. B-52s and the Northern Alliance's Soviet era tanks.

There is a reason that SOF were called upon to lead Operation Enduring Freedom, and why SOCOM will be called upon to lead future operations to destroy terrorist networks. The SOF operator is distinguished from other military personnel by his language capabilities, his extensive overseas experience, his ability to work closely with indigenous forces and to train them, his ability to blend into the fabric of the society in which he operates, his independence and maturity, and an unparalleled degree of training. These Americans truly are one of a kind – each one. That is why there are so few of them. They cannot be mass produced. Nor can their equipment. They are one of the nation's most scarce and precious resources, and they should not be employed casually.

But, when we do call on them, as we saw in Afghanistan, and as we have seen time and again in other military operations – we know that the interests of the nation will be well served.

SOF demonstrated their myriad of capabilities during Operation Enduring Freedom – within Afghanistan and simultaneously throughout the rest of the world. While Army Special Forces conducted unconventional warfare with the Northern Alliance to destroy the Taliban's warfighting capability, other Army and Navy SOF were conducting special reconnaissance and direct action to destroy Al Qaeda. Army Rangers demonstrated their strategic reach and prowess in night operations. Air Force and Army special operations aviators performed their intrepid work under conditions where investments in specialized training and equipment produced capabilities unique to SOF. Air Force Special Tactics airmen transformed the role of SOF by integration of every U.S. Service's airpower into the operation – their unique ability to “rack and stack” multiple types of aircraft, procedures, and communications frequencies and to bring precision and “dumb” ordnance “danger close” and on target proved crucial to halting and reversing Taliban offensives throughout the countryside, and to crushing Taliban resistance around key cities. The result of this combined push by SOF was a Taliban uprooted and an Al Qaeda on the run.

Other SOF capabilities have assumed a newfound importance. We all have heard the term “winning hearts and minds.” SOCOM’s Civil Affairs men and women are deployed worldwide long before hostilities erupt. They also remain long after the guns fall silent to help rebuild the instruments of effective governance. While the bulk of the mission in Afghanistan has now fallen to the conventional military, the most important part – winning the peace – still is in the hands of the Civil Affairs operators who are working with the U.S. Agency for International Development and the State Department to rebuild a society torn by war and frayed by fanaticism. Stability of the Karzai government, promoted through consistent and measurable improvement in the quality of life for the Afghan people, is essential to U.S. national security. The work of the international community, and SOCOM’s Civil Affairs personnel, are crucial to that effort.

The work of Civil Affairs in Afghanistan also sends an important message to the Muslim world. Our quarrel is not with Islam. Our fight is with terrorists and those who support or harbor them. By removing the Taliban, we have made life livable, once again, for the Afghan people. The same will be true for the people of Iraq. It already is the case for the southern part of Iraq today, as humanitarian aid has begun to flow in. That is a message that the Muslim world needs to hear and understand.

Which brings me to another invaluable part of the Special Operations Community, the servicemen and women in our Psychological Operations detachments. These people are spearheading U.S. efforts in a war of words and a battle of ideas. Their success is fundamental to victory in the war on terrorism. After all, we can spend endless time and effort chasing terrorist operatives. Unless we can address the root causes of terrorism, the conflict in which we are now engaged will never end. On a strategic level, PSYOP programs offset the shrill and distorted propaganda of our adversaries by offering alternative sources of information to those denied the basic rights of freedom of speech and expression. At the tactical level, SOF capabilities to transmit radio broadcasts, to distribute leaflets and to use loudspeakers provide opportunities for enemy soldiers to surrender and prevent civilians from getting in harm’s way.

Now, despite the fact that SOCOM was deeply committed to the Afghanistan theater, in support of CENTCOM, the Command proved that the United States could mount other major SOF-run operations concurrent with, and shortly following, Operation Enduring Freedom. Some of those efforts are ongoing today. Activities in the Philippines, Colombia, Cote d’Ivoire, and Georgia were a few examples. Today, with Special Operations Forces heavily committed in Iraq, there nevertheless are concurrent operations being run in Afghanistan, Yemen and the Horn of Africa, and SOF advisors scattered throughout numerous other countries conducting indigenous training and facilitating the flow of tactical information for host-nation run operations against terrorist groups.

### *Transforming USSOCOM*

That said, we are learning a number of lessons from the war on terrorism. Accordingly, the Department of Defense has begun a significant “retooling” of

USSOCOM to enable the Command to lead the war effort in an even more effective manner. Congress will see that re-engineering effort manifested in the President's Fiscal Year 2004 Budget Request. Perhaps the most profound change is a shift in expectation by the Department that USSOCOM will no longer serve as primarily a *supporting* command, but rather will plan and execute certain key missions as a *supported* command.

The change from supporting command to supported command will necessitate some significant funding changes and the addition of certain types of personnel and units. Additionally, USSOCOM will look to move certain collateral SOF missions – either in part or in full – to conventional branches of the military in order to free up special operators for their primary mission – to wage war against terrorists.

In the President's Budget for Fiscal Year 2004 (FY2004), an increase of about 47 percent has been proposed for USSOCOM, totaling approximately \$4.5 billion. This increase includes an additional \$391 million for operations and related expenses, and about \$1.1 billion in procurement of critical equipment. These increases facilitate the addition of 2,563 personnel in critical mission areas. Military personnel costs which are included in the budgets of the Military Departments total another \$1.2 billion.

Some of the increase in funding will allow SOF to forward deploy into, and sustain operations in, areas where terrorist networks are operating. Additional funding also is devoted to investments in critical "low-density/high-demand" aviation assets that provide SOF with the mobility necessary to deploy quickly and to execute their missions quickly, safely and with the necessary low, or invisible, profile.

Additional funding is requested to fix command and control shortfalls in both equipment and personnel that could have potentially diminished USSOCOM's ability to simultaneously prosecute a variety of expanded missions. The increases will allow USSOCOM to provide both a strategic planning and operations capability for missions launched from the United States, and to run operations via the several Theater Special Operations Commands (TSOCs) that are now dual-hatted, with responsibilities to both the regional combatant commander and to USSOCOM. In addition, several of the TSOCs will receive additional personnel and equipment to support the continuing war-level pace of the activity in theater. For example, we plan to begin forward basing of additional SOF units and mobility platforms in CENTCOM, including Navy SEAL teams and Army and Air Force SOF aviation units, although specific basing decisions have not been finalized. In toto, the TSOCs will receive 232 additional personnel and additional command, control and communications equipment.

Also, we are allocating funding to sustain equipment that was acquired in the Fiscal Year 2002 supplemental. Some additional equipment and sustainment costs associated with transfers of personnel from the service departments to USSOCOM will also be covered by the increases in funding.

### *The Equipment*



Several critical equipment acquisitions are being put into motion with FY2004 increases. The budget will mitigate a shortage of critical aviation assets, including through the life extension or modification of existing platforms. Specifically, USSOCOM will begin modification of 16 additional CH-47s into MH-47Gs, fund an MH-60 service life extension program which will improve the avionics and give those airframes another 20 years of life, accelerate the MC-130H aerial refueling modifications, continue the modification of 4 C-130s into AC-130U gunships, and weapons kits and ammunition for 10 additional MH-60 Defensive Armed Penetrators. I will note that the MH-47E has proven a workhorse in offensive combat operations, but that the handful of available platforms have taken a beating. More than half of the MH-47 fleet has been destroyed or damaged at some point, and there is a great deal of "tired iron" in the USSOCOM inventory at this stage. When you measure your assets in 1's and 2's or even 10's, as USSOCOM does, the loss of a single system can have far-reaching effects. Fixing USSOCOM's mounting aviation problems that are accruing simply due to the high OPTEMPO of counter-terror operations is a top priority within this budget. And because we know to expect future loss of systems and platforms, we have begun planning an attrition reserve for the Command.

There is other additional funding which allow the procurement of new capabilities. The FY2004 budget begins a long overdue modernization of PSYOP media production, broadcast and leaflet delivery systems. U.S. PSYOP capabilities have proven their worth in Afghanistan, and now in Iraq, and we are going capitalize upon the recent revolution in telecommunications technology by providing the Command with a research and development program to demonstrate the utility of technologies such as satellite radio and UAVs for PSYOP messaging.

### *The People*

I mentioned earlier in my testimony the exceptionally high caliber of individual who serves as a SOF operator. Recruiting, training, and retaining this kind of person is a constant challenge for the Department of Defense and the Command. Increases in funding will allow USSOCOM to increase by an additional 2,563 personnel in FY2004 for an end strength of 49,848 personnel. About one-third of the uniformed personnel are in reserve component units.

In addition to personnel "adds" for key operational planners in Tampa, and with various subunified commands (SOCs), additional manpower is applied to existing units to increase SOF's responsiveness and provide continuous forward-staged assets. Many of the additional numbers will support the Army's aviation crews who specialize in flying combat troops behind enemy lines. Additionally, more than 1,200 forces will be forward-deployed operational, support and command and control elements.

The increases will also allow for the addition of new units, including the establishment of a unit to coordinate trans-regional PSYOP activities as well as additional Civil Affairs units (an asset stretched very thin by current OPTEMPO), support units and an aviation unit. In FY2004, USSOCOM will add a reserve Civil Affairs battalion, an

active Civil Affairs company, an active MH-47 aviation battalion, and an active PSYOP company. In FY2005, USSOCOM plans to add an active Civil Affairs support company, an active regional PSYOP company, four reserve regional PSYOP companies, and two special operations support companies.

Recruiting, training and retaining SOF will not be without challenges. Several initiatives were implemented over the past year to improve the effectiveness of these efforts. While we continue to track this issue closely, and are particularly watchful of retention metrics, our analysis to date indicates that the Command will have the right numbers to sustain the SOF forces the nation needs. Training instructors and the number of training slots available have increased for Army Special Forces, Civil Affairs and PSYOP training. A recruiting initiative was launched in which new Army recruits can sign up for Special Forces directly, rather than awaiting selection from a conventional unit. This is an option that has not been possible since 1988. Also, special pay and bonuses were implemented to improve retention in highly specialized areas and units.

#### *Possible Transition of SOF Mission Tasks to Non-SOF Forces*

Additionally, two other issues need mention: the possible transition of certain mission tasks traditionally done by SOF to other military forces, and the evolving operational relationship between USSOCOM and the Marine Corps.

The question about a possible trade-off between effectiveness in execution of "core" SOF missions and fulfilling all the responsibilities set out for USSOCOM in Title 10 is not new. Still, the centrality of SOF in the war on terror, and USSOCOM's lead military role, again give that question renewed importance. Simply put, should SOF be responsible for certain mission tasks during wartime when other parts of the military can assume those roles?

It is not a question of whether certain tasks are essential for the U.S. military to undertake and perform to the highest standard, but rather whether SOF have to perform that mission in all cases. One of the primary purposes of explicitly outlining the missions of USSOCOM in statute was to ensure that these particular missions were the responsibility of a single, unified entity.

The combination of a joint environment, and the specialized capabilities that are hallmarks of SOF, have made USSOCOM an innovator or incubator for new techniques, missions, organization, and technologies. Over time, as the big services have grasped the utility of USSOCOM innovations, the entire U.S. force structure has benefited. Much of what is developed for SOF becomes the norm in the conventional military as missions and technologies evolve. An example is Theater Search and Rescue, which is a core competency and a USSOCOM mission, but one which has been adapted and assumed by many other parts of the military. Air Combat Command, for example, retains its own theater search and rescue capability that is fully supported by the Air Force and does not depend on USSOCOM.

As the process of innovation and dissemination continues, and the missions and capabilities that were once unique to SOF become evident elsewhere in the military, it is reasonable to reexamine whether primary responsibility for certain tasks can be divested. We do not have an answer to this question, yet, but I assure the Committee that the Office of the Assistant Secretary for SO/LIC – together with the Command – is looking at this very hard.

### *The Marine Corps*

The relationship between the Marine Corps and SOF continues to evolve in a very healthy direction. For the first time in history, USSOCOM and the Marine Corps have established a construct for joint warfighting. A Marine detachment is in a one-year proof of concept phase that began last fall. On October 1 of this year, we expect it will be fully integrated into a Naval Special Warfare Squadron and serve there on a rotating basis. Additionally, last year, SOF and the Marines began joint wargaming exercises called “Expeditionary Warrior,” which focuses on cooperation (with naval support) in combating terrorism and counter-proliferation contingencies.

As USSOCOM assumes its role as a supported command in the war on terrorism, and can draw on all services’ assets in a theater of operation, the joint capability being established between the Marines and SOF will undoubtedly grow. We can expect that we will realize ways in which such cooperation is possible or even essential.

### *In Closing...*

We are making progress, and are “taking the fight” to terrorist organizations wherever we can find them. SOF are in the vanguard of that effort, having proved their mettle, and value to the nation, during Operation Enduring Freedom and numerous other operations. That said, the pace and intensity of our operations cannot be diminished or relaxed in any way, at any time.

If given any respite, al’Qaida and other groups will rebuild themselves and strike in ways ever more horrific. Each element of SOF has a role to play in the sustained campaign against al’Qaida and other terror networks or states, from deconstruction of terrorist cells to reconstruction of societies in Afghanistan, and in a future, liberated Iraq.

Although this posture already has stretched and tested the limits of the current force, the Administration is bringing to bear additional resources, is forging new partnerships, and may transition some missions to ensure that SOF resources are not depleted during the global campaign. With that assessment, and with a request for your support for both the President’s FY04 budget and the Supplemental – which is urgently needed by the Command. I am prepared to take any questions that you might have.

STATEMENT OF  
HARRY E. SCHULTE  
ACQUISITION EXECUTIVE  
UNITED STATES SPECIAL OPERATIONS COMMAND

Mr. Chairman and distinguished Members of this Subcommittee, it is an honor and privilege to report to you on United States Special Operations Command (USSOCOM) programs.

SOF remain the most capable and ready force in the world today. We have seen great change in our Nation as America takes action against terrorism. As you know, USSOCOM has been a key player in that response. This statement addresses two critical challenges and provides an overview of USSOCOM's Fiscal Year 2004 (FY04) budget request. The two challenges addressed are fighting terrorism on a global scale and transformation.

First is the war against terrorism on a global scale. USSOCOM has been at the forefront of this fight since initiation of combat operations following the September 11th attacks. Given the character of this war and the stakes involved, SOF is on the offensive. The aspect of today's international terrorist is far different than in the past, as terrorists now have global reach, infrastructure, and significant resources. The attacks on our Nation on September 11, 2001, clearly demonstrated that determined terrorists will go to any lengths to inflict catastrophic losses on Americans, regardless whether they are civilians or military personnel. Of greater importance is the fact that these terrorists have chemical, biological, nuclear, and high-yield explosive weapons and the desire to kill as many Americans as possible and undermine our Nation's interests and influence around the world.

SOF play a vital role in combating and defeating global terrorism, by disrupting terrorist organizations and bringing their members and supporters to justice ... or by taking justice directly to them. The mission of USSOCOM is expanding to planning direct combat missions against terrorist organizations around the world and executing those missions as the supported Command, while maintaining the role of force provider and supporter to the Geographic Combatant Commanders. To meet this challenge, USSOCOM must establish command and control infrastructures which complement the Geographic Combatant Commanders and invest in programs and systems improving SOF's speed, agility, precision, lethality, stealth, survivability, and sustainability. USSOCOM must also be forward-deployed for rapid response. The requirement to plan, synchronize, and execute operations on a global scale necessitate a globally capable SOF ready for full spectrum integrated operations.

Full spectrum integrated SOF are the refinements that must occur to tailor SOF capabilities for the war on terrorism. These SOF capabilities will ensure greater operational agility, flexibility and mobility, sufficient global command and control, focused intelligence, signature reduction, and a collaborative planning environment that facilitates simultaneous multi-echelon planning. Additionally, SOF capabilities must continue to address other national and military strategies, including homeland defense and forward deterrence, swiftly defeating the efforts of adversaries and decisively winning lesser contingencies.

All personnel of USSOCOM - Active duty, Reserve Component and civilians, are engaged in this multi-front global war on terrorism (GWOT). The battlefield successes in this campaign have proven again and again the foresight of Congress in the creation of USSOCOM. USSOCOM's organizational flexibility and streamlined acquisition and resourcing authorities continue to allow unequalled response to the needs of our operators. The capability of



conducting joint operations is enhanced by synchronizing SOF, which include Army Special Operations Aviation, Special Forces, Rangers, Civil Affairs, and Psychological Operations forces; Air Force Special Operations Aviators and Special Tactics Squadrons; and Navy Sea, Air, and Land (SEAL), SEAL Delivery Vehicle Teams, and Special Boat Teams.

The continuing action in Afghanistan ... and now in Iraq ... is a great example of how joint warfighting has evolved from the Goldwater-Nichols legislation as a powerful and precise tool to support our Nation's vital interests. Daily Civil Affairs' teams and other SOF continue to play an active role in Afghanistan to ensure we win the peace. Our activities in Operation Enduring Freedom have given the world a much clearer insight into the skills, dedication, and power across the spectrum of America's SOF, specifically as part of a larger joint and interagency team - each bringing their specific skills and capabilities to the team. The ability to win across the spectrum of military operations requires seamless joint teamwork and USSOCOM is privileged to team with the Services to create the best warfighting capability the world has seen.

USSOCOM's other opportunity is transformation. The hallmark of SOF is that they are always open to change and "out of the box" thinking. Transformation embodies our SOF core values ... integrity, courage, competence, and creativity. The success of change and transformation is the ability to maintain the goodness of the past, while taking calculated risks that promise competitive advantages on the battlefield for our future forces. We must change to ensure that we have maximized the ability of the human to think and problem solve, while taking advantage of the rapid pace of technology. Transformation is not about equipment, it is about a holistic approach producing sweeping advances for the individual, to the organization structure, to the appropriate application of technology to build the right capability at the right time to defeat any threat ensuring the safety of our

Nation now and into the future. Transformation of SOF is a journey, not a destination and there is no mark on the wall that will indicate we are finished transforming.

While SOF activities remain constant, the context of how and the manner in which they are executed has changed significantly. Traditionally, SOF were employed as a force multiplier to wage war against other nation states. Traditional warfare focused on the destruction of large massed armies, navies and air forces. Supporting intelligence communities developed capabilities to locate and track these large enemy combat elements. In traditional conflicts, the main effort was expended on the physical destruction of the enemy's military capability during large battles. USSOCOM is transforming intelligence and interagency capabilities not to locate and destroy large enemy combat elements, but to locate and track individual terrorists across the globe and conduct small surgical operations with minimal risk to the employed force.

In addition to the war on terrorism, SOF are still committed to the Geographic Combatant Commander's theater security cooperation plans. These include the European Command (EUCOM)-led campaign in Bosnia and Kosovo, the Pacific Command's (PACOM) support to combating terrorism in the Philippines and exercises with our allies in the Republic of Korea, Southern Command's (SOUTHCOM) narco-terrorism programs, providing crucial SOF for Central Command's (CENTCOM) combat operations including OPERATION ENDURING FREEDOM, as well as cooperative efforts with Joint Forces Command (JFCOM) and the newly established Northern Command (NORTHCOM).

#### **STRATEGY**

USSOCOM's broad, yet unique, mission areas and capabilities allow us to make a number of important contributions to the National Security Strategy, especially in the War on Terrorism. Although SOF cannot address every crisis, we provide policymakers an expanded set of options for rapidly

resolving strategic crises with relatively limited resources, fanfare, and risk. SOF's ubiquitous presence as "Global Scouts" serves to assure our allies and friends of the United States' resolve. SOF's selective and integrated participation in support of Theater Security Cooperation Plans (TSCP) to include: Joint Combined Exchange Training (JCET), Humanitarian Demining (HD), Humanitarian Assistance (HA), Narco-Terrorism (NT), and Foreign Internal Defense (FID) programs which provide tangible benefits in support of war on terrorism objectives and Geographic Combatant Command strategies while building rapport with our friends and allies.

The global presence of SOF and their unique capabilities dissuade potential adversaries by disrupting their planning, while providing the President and Secretary of Defense a wider array of options for dealing with potential adversaries. Forces organized, trained, and equipped to execute the SOF principal missions of combating terrorism and counterproliferation of weapons of mass destruction also provide critical deterrence against adversaries that might contemplate producing or employing these weapons against the homeland or our friends and allies. SOF can deter threats and counter coercion through the deployment and employment of forces specially tailored to counter adversaries' capabilities through direct and surrogate means.

By operating "in the seam" between peace and war, SOF can address transnational and asymmetric threats through direct military means or concerted action with conventional military forces or other government agencies. SOF help shape the pre-conflict environment, setting the conditions so they are favorable to U.S. objectives and provide a strategic economy of force in areas of the world left uncovered by the commitment of conventional forces to other priorities.

#### **EXPANDED ROLE OF USSOCOM**

While our Nation is at war, we realize this war is unlike any other ever fought. It is a war without formal declaration, concrete resolution, nation state boundaries, and against adversaries willing and able to strike directly against our homeland or our citizens abroad. It is a potentially interminable war in which our adversaries are likely to use weapons designed to cause catastrophic injury to our citizens and our way of life.

The nexus of the Department of Defense's global war on terrorism effort is at USSOCOM. USSOCOM's strategy encompasses the entire spectrum of special operations missions, capabilities and methods; then incorporates conventional capabilities, as necessary, for mission success. USSOCOM's nine legislated activities remain relevant in determining our missions and activities in the fight against terrorism. To accomplish this, USSOCOM is employing SOF simultaneously worldwide through focused deployments to priority regions in order to prepare the battlespace, both physically and psychologically, and set the conditions for global war on terrorism operations. As the situation develops and terrorist targets are located, operations are conducted to further identify and acquire the target, followed by combat operations. The overall intent is to seize and maintain the initiative through constant pressure against known or suspected terrorist organizations and infrastructure.

As USSOCOM's role expands, this will generate changes in our manpower, organizational structure, facilities, equipment, and special programs relating to the expanded responsibilities. As the command assesses the specific changes needed to meet these expanded operational requirements, SOF will continue to collaborate with the other Combatant Commands and inter-agency partners that have key information operations (IO) supporting responsibilities in order to accomplish our changing mission in a responsible, coordinated manner.

#### COMMAND RELATIONSHIPS

USSOCOM's headquarters organization and activities are changing dramatically to fight the war on terrorism. As the supported Commander for planning the Department's global war against terrorist organizations, USSOCOM will plan and selectively execute combat missions against terrorists and terrorist organizations around the world. In order to most effectively enhance our ability to respond as both a Supported and Supporting Command, we are formulating the integration of our intelligence, operations and planning, and analysis divisions into a single facility. The effect will be a synergy of talent into a single entity which will significantly enhance and focus our unique war fighting capabilities.

USSOCOM's planning efforts will focus on the development of recommended courses of action to the Secretary of Defense and the Chairman, Joint Chiefs of Staff. USSOCOM is also developing the processes and organizations required to collaboratively draft, coordinate, and globally synchronize plans and operations. These forces could include any of our special operations forces or part of the Theater Special Operations Command (TSOC), but may also include conventional forces, as necessary.

During the execution phase, USSOCOM will conduct detailed planning and execute the approved courses of action using the TSOC or a Joint Task Force or Joint Special Operations Task Force as our operational and tactical coordinator. This is a significant and transformational change in strategic military command and control and will require a major adaptation of USSOCOM headquarters and the Geographic Combatant Commanders' TSOCs.

The Geographic Combatant Commander's area of responsibility in which the operation is to be executed supports our request for forces by providing operational control of the forward deployed forces necessary to execute the approved courses of action, in accordance with the Department's deployment order. USSOCOM will be prepared to conduct follow-on operations based upon exploitable intelligence and operational opportunity.



USSOCOM has formed a collaborative planning environment through the Geographic Combatant Commands' staff and interagency liaisons. The collaborative planning identifies interagency requirements, issues planning guidance as appropriate, reviews, validates, and submits plans with recommended delegation of command relationships for execution for Departmental approval. This command relationship recommendation may not always recommend USSOCOM as the supported command, but may in fact, recommend the Geographic Combatant Commander as the supported Command and USSOCOM will remain in its traditional role as supporting command. In that instance, during planning, the Geographic Combatant Commands' staff (designated as the supported command for execution) determines the forces, tactics, methods, procedures, and communications for employment. During execution, the Geographic Combatant Command's staff executes the approved courses of action, collaborates with USSOCOM, and provides post-operation assessments. The Geographic Combatant Command will be prepared to conduct follow-on operations based upon exploitable actionable intelligence and operational opportunity.

USSOCOM's traditional role of a "supporting" command; responsible for providing trained and equipped SOF to the Geographic Combatant Commanders is thus a "supported command for planning" and, when necessary, "supported command for execution" within the Geographic Combatant Commands' areas of responsibility. Under these circumstances -- supporting or supported for execution -- a flexible command relationship structure that exploits the command and control capabilities already present in the Geographic Combatant Commanders' staff. This will enable us to prosecute missions supporting the war on terrorism will allow USSOCOM to focus our energies.

#### **TRANSITION AND SHARING OF SOF EMPLOYMENT TASKINGS**

SOF are traditionally small, highly trained, specifically organized, and uniquely equipped to perform missions conventional forces are not trained, organized, or equipped to perform. To better focus USSOCOM's

efforts in the war on terrorism, the Department and USSOCOM are conducting reviews of the SOF principal missions and collateral activities in order to identify the mission employment taskings currently performed by SOF that could be transitioned or shared with our conventional force partners or other governmental agencies. USSOCOM's measuring stick is those missions, tasks, and activities as they pertain to access, intelligence development, and operational preparation to prosecute combat operations in the war on terrorism. SOF routinely consider leveraging conventional forces and interagency partners to perform certain missions. However, if a mission task does not align directly or indirectly with the war on terrorism, or provide access to a significant area or objective, SOF have the ability to transition or load-share these tasks with conventional forces. Examples of this load-sharing are the Georgia Train and Equip missions and personal security detail for Afghanistan's President Karzai, which were transitioned to conventional forces or other government agencies -- seamlessly. Future SOF deployments should identify at the time of deployment a conventional force to be prepared to assume the mission taskings as they are identified and when the unique capabilities of SOF are no longer required, both operational and support. The transition of SOF employment taskings to a conventional force, while prioritizing and focusing all SOF deployments, in coordination with Geographic Combatant Commanders, is essential to our continued success in planning and executing the war on terrorism.

#### **STRATEGIC CHALLENGES AND RISK**

We know that current terrorist networks are linked with non-state actors with very different local strategies but mutually self-supporting goals. These nodes operate across international boundaries, spanning and circumventing current geographic constructs. The imprecise nature of terrorist goals and the ambiguous international environment have nullified traditional responses. This dangerous mix catapults the need for an

extremely sophisticated joint, interagency, combined and coalition strategy to unparalleled levels, which currently challenge our Nation to unprecedented levels.

Global access is vital to the preservation of U.S. national security and SOF must have the ability to access and operate anywhere in the world, in any mission environment, from benign to hostile. SOF maintain access and an understanding of local issues through geographic orientation, cultural acuity, and continued forward presence and security cooperation. Although theater security cooperation events provide SOF access to most parts of the world, SOF must retain the ability to operate where U.S. forces may be unwelcomed or opposed through unconventional warfare methods. Potential adversaries are acquiring weapons and developing asymmetric capabilities to deny United States forces access to critical theaters of operations in a crisis. As first responders -- global scouts, pathfinders, and door openers -- SOF set the stage for follow on forces.

The risks facing USSOCOM include Operational Risk during preparation of the battlespace encompassing Force Management Risk, and Future Challenges Risk. Operational Risk is the ability of a force to achieve military objectives in a near-term conflict or other contingency. Force Management Risk is the ability to recruit, train, retain, and equip sufficient numbers of quality personnel and sustain the readiness of the force while accomplishing its many operational tasks. And, lastly, Future Challenges Risk, refers to the ability to invest in new capabilities and develop new operational concepts needed to dissuade or defeat mid- to long-term military challenges.

Like the Services, SOF have reduced operational risk by reallocating resources from its modernization and recapitalization accounts to fund current readiness. Nevertheless, SOF will require significant enhancements in capability, capacity and speed of response enhancements to meet all

priorities. SOf may have to accept operational risk in some areas in order to build new operational capabilities. Some key issues associated with operational risk include: sizing the force to conduct effective operations, optimizing basing to support strategic objectives, and improving SOf strike and mobility capabilities.

In many respects force management risk is the most critical problem facing SOf. The special operations community must retain its experienced and seasoned personnel to gain the significant return on investments made in the areas of assessment, selection, training, and education. For example, today's Green Beret is the only operational specialty that requires a foreign language for qualification - a critical skill that must be retained as we posture for future operations. Some key issues associated with force management risk include: retention of mid- and senior- grade personnel and growing the force to meet current as well as emerging operational requirements.

Dealing with future challenges will require force transformation - where these challenges can be overcome by using fundamentally different organizations, tactics, techniques and procedures than those used by today's forces. Some key issues associated with Future Challenge Risk include improving trans-regional information capabilities to support global operations; building a linguistically, culturally and ethnically diverse force; improving capabilities to operate for extended periods in anti-access environments; providing force protection in adverse environments; improving ground-directed fire support; and improving capabilities to operate in urban environments.

#### **TRANSFORMATION AND REORGANIZATION**

SOf must continue to operate effectively in joint, combined, and interagency environments while also fusing capabilities that reflect U.S. political, military, economic, intellectual, technical, and cultural

strengths into a comprehensive approach to future challenges. USSOCOM, therefore, embraces the process of transformation in a disciplined manner that allows the command to move towards its goal of full-spectrum, integrated SOF. Our use of full-spectrum, integrated SOF will allow us to tap into diverse areas, such as commercial information technologies, utilization of space, biomedicine, environmental science, organizational design and commercial research and development. All aspects of SOF – the organization, force structure, platforms, equipment, doctrine, tactics, techniques, procedures, and missions – must continuously transform to meet the needs of the nation and seize the opportunities manifested by change.

As we develop the tools to conduct our expanded mission in the fight against terrorism, USSOCOM must transform our headquarters into one that includes the traditional train, organize, and equip mission with the capability to plan and execute the warfight against terrorism. Our component commands face this same challenge. Some areas already being addressed include the growth in our warfighting staff to build an organization oriented on the expanded mission of an operational headquarters without degrading the necessary work of our resourcing and acquisition headquarters. USSOCOM has also developed a 24-hour joint operations center with the connectivity to work with the Geographic Combatant Commanders and the TSOCs and a Campaign Support Group from a myriad of commands and interagency partners. In the near future we will see these activities consolidated into a "state of the art" warfighting center.

The 21st century SOF warrior – selectively recruited and assessed, mature, superbly trained and led – will remain the key to success in special operations. These warriors must be capable of conducting strategic operations in all tactical environments – combining a warrior ethos with language proficiency, cultural awareness, political sensitivity, and the ability to maximize information age technology. We must also have the intellectual



agility to conceptualize creative, yet useful, solutions to ambiguous problems, and provide a coherent set of choices to the Combatant Commands or Joint Force Commander.

People will always remain the most important component of SOF capability. However, future SOF will use technological advances more effectively. Technology improvements will allow commanders to track and communicate discretely with SOF in the field. Improvements in unmanned vehicle technologies will provide better precision fire, force protection, personnel recovery, and logistics support. SOF must develop new competencies and enhance existing ones in support of critical national requirements, including the ability to locate, tag, and track mobile targets and support trans-regional information operations.

USSOCOM is focused on providing the most accurate and complete intelligence support to our tactical commanders and deployed forces. SOF does this by leveraging national, theater, and Service intelligence resources with our SOF-peculiar systems and intelligence professionals.

USSOCOM continues to transform our PSYOP force structure and capabilities to improve our support to Geographic Combatant Commander's influence initiatives, and on-going military operations. Lessons learned from multiple contingency operations, including OPERATION ENDURING FREEDOM, identified a requirement to increase our PSYOP force structure to meet the demands of the Geographic Combatant Commanders. The Department of the Army agreed to crosswalk the necessary manpower in order to activate two additional Active Duty and four Reserve Geographic PSYOP Companies. To modernize our PSYOP force we are proposing an Advanced Concept Technology Demonstration (ACTD) that will explore emerging technologies to increase the dissemination range of our PSYOP products into denied areas and develop state of the art PSYOP analytical planning tools. USSOCOM is also modernizing our

PSYOP EC-130E COMMANDO SOLO television and radio broadcast aircraft by cross-decking the EC-130E into the newer EC-130J model.

USSOCOM has also developed a new construct in joint warfighting with the fusion of a Marine Corps USSOCOM Detachment into one of our Naval Special Warfare Squadrons. Naval Special Warfare Command (NSWC) continues to pioneer U.S. Navy warfighting capabilities to support special operations in the War on Terrorism. NSWC is the lead agent on the establishment of the SOF module on the Littoral Combat Ship (LCS) and evaluating SOF modifications for U.S. Navy rotary wing programs. In addition, NSWC's transformation efforts include unprecedented experimentation in the new SSGN conversion effort. SOF's Naval Special Warfare component is also collaborating with the Department of the Navy to pursue technologies and concepts to find, fix, and finish non-state threats such as the global War on Terrorism.

USSOCOM and the Marines have signed an agreement to establish the initial Marine Corps force contribution to SOF, which will jointly train and deploy with naval special warfare in the Spring of 2004.

Finally, and most important, the improvement of SOF training, education, and experience contributes to the development of SOF's capability. Doctrine, organization, and materiel factors have additive value to the force; leadership and personnel factors, however, exponentially multiply investments in doctrine, organization, and materiel. As training, education, and experience influence the quality and effectiveness of leadership, these variables have the greatest long-term effect on SOF capabilities. In order to maintain strategic flexibility and maximize the likelihood of operational success, SOF will increase their commitment to "train for certainty, educate for uncertainty."

USSOCOM's expanded mission and organizational changes constitute a new vector that will require a continual effort to refine our Transformation Roadmap based on this new azimuth. USSOCOM will be a hybrid of the

Geographic Combatant Commanders and a specified command for Special Operations support. More than ever, our transformation is truly a process, not a destination.

#### **BUDGET AND ACQUISITION**

One of the strengths of the command, thanks to the wisdom of Congress, was the establishment of a separate Major Force Program (MFP), MFP-11, for SOF along with the requisite acquisition and research, development, test and evaluation (RDT&E) authority. It is a powerful tool that allows us, as you know, to quickly meet the soldier, sailor, or airman's equipment needs. This is accomplished by a world class acquisition center at Tampa, made up of folks who live by some very specific and exacting acquisition principles. Our fundamental acquisition strategy is to rapidly field the 80 percent solution while working with the warfighters and industry to continue to address the last 20 percent.

USSOCOM's expanded role in the war on terrorism has resulted in expanded resources as the Department recognized the challenges confronting SOF and the Nation. USSOCOM's FY04 budget request is \$6,735 million, 1.8 percent of the Department of Defense budget. A summary and some highlights of SOF's FY04 request is provided below.

#### **Military Personnel**

Today, the relative health of the special operations community remains strong. The long-term stabilization of our health depends upon continued efforts to ensure our people experience a quality of life commensurate with their hard work and their dedication to duty. Increased pay and allowances and special pays are crucial to the continued health of our community. It is imperative that we continue to improve military pay and allowances and fund the Reserve Component military pay for additional schools as well as training days necessary for Reserve Component SOF Military Personnel (MILPERS) requirements. Congressional support is a powerful signal to our

deserving men and women and will have a tremendous impact on our future health and readiness.

The total SOF end strength for FY04 will grow to 49,848 manpower resources with about one-third of our military manpower in Reserve Component units. Thanks to the Department's recognition of a need for more SOF, and the Services' cross-walking end strength to SOF, we will see an end strength increase of 3,869 over the next five years.

This end strength growth primarily supports the manning requirements to wage the global war on terrorism. The increases are focused on fixed and rotary-wing aviation, SEAL Teams, Civil Affairs (CA), PSYOP, TSOCs, and support to USSOCOM as the supported combatant commander in the war on terrorism. While USSOCOM budgets for SOF personnel, the Services execute the funds. For FY04 our MILPAY request totals \$2,210.8 million.

#### **Operation and Maintenance (O&M)**

Operation and Maintenance (O&M) is the heart of maintaining SOF operational readiness. O&M includes the day-to-day costs of SOF unit mission activities, such as civilian pay, travel, airlift, special operations-peculiar equipment, equipment maintenance, minor construction, fuel, consumable supplies, spares and repair parts for weapons and equipment, as well as the headquarters functions of USSOCOM and its Service components. Our FY04 O&M request is \$1,994.1 million. An additional \$12 million supports SOF from MFP-3 (command, control, communications and intelligence [C4I]) O&M funds.

Operating forces include the necessary resources for SOF tactical units and organizations, including costs directly associated with unit training, deployments, and participation in contingency operations. Resources support civilian and military manpower, SOF peculiar and support equipment, fielding of SOF equipment, routine operating expenses, and necessary facilities.

#### **Procurement**

Along with the authority to budget and program for SOF activities, USSOCOM also has the authority to develop and acquire Special Operations peculiar equipment to prepare SOF to carry out their assigned missions. This provides the warfighter with the tools necessary to fight not only the most committed industrial age power, but also the means to fight entities that would and could wield influence through terror by any means. USSOCOM's FY04 Procurement request is \$1,978.3 million, an increase of over \$1 billion over the amount appropriated in FY03. Speaking of FY03, we would like to thank Congress for the procurement increases received - over \$137 million - including the transfer of funds from the Defense Emergency Response Fund.

The current state of SOF capabilities is strong, but to meet the evolving capabilities of potential adversaries, we must invest now to ensure reliable support for the Defense Strategy. USSOCOM's aim in pursuing technological transformation is to guarantee our forces remain relevant to any fight, and ensure we minimize risk to our Nation's vital interests.

To enhance our force projection capabilities, we must continue to invest in programs to improve strategic mobility, force protection, research and development, and information dominance.

Our Air Force Special Operations rotary-wing capabilities must remain safe, sustainable and relevant. USSOCOM is working to ensure the airworthiness and defensive system capabilities of our MH-53 helicopters to allow them to fly in the threat environments they face on the battlefield.

The heart of our future rotary wing capability as we transform Air Force special operations to the CV-22 is the rotary-wing upgrades and sustainment funding provided for critical improvements to our Army special operations aircraft. These aircraft must be capable of operating at extended ranges under adverse weather conditions to infiltrate, reinforce, and extract SOF. The FY04 budget provides ongoing survivability, reliability, maintainability, and operational upgrades as well as procurement and



sustainment costs for fielded rotary wing aircraft and subsystems to include forward-basing of MH-47 helicopters. In FY04, the Department made a concerted effort to mitigate our most pressing problems associated with SOF low density/high demand rotary wing assets. In particular, the MH-47 inventory was increased by 16 aircraft in FY04 by diverting CH-47D aircraft from the Army's service life extension program (SLEP) production line to the SOF MH-47G production line to help alleviate USSOCOM's critical vertical lift shortfall due to battle damages. The command is grateful to the Army for their support. The MH-60 fleet begins a major program in FY04 to extend its useful life, which will significantly upgrade our MH-60 fleet. Improvements to both fleets will enhance SOF's ability to conduct both medium and long range penetration into denied or sensitive areas. These programs will keep our Army rotary wing relevant well past 2020.

The command is committed to the CV-22 aircraft and its unique capabilities. We will continue to assure the CV-22 is safe, reliable, and maintainable for SOF forces. The long-range, high speed, vertical lift CV-22 fills a long-standing SOF mission requirement not met by any other existing fixed or rotary wing platform. The Navy is the lead Service for the joint V-22 program and is responsible for managing and funding the development of the baseline V-22, Osprey. The Air Force will procure and provide the fielding of 50 CV-22 aircraft and purchase service common support equipment for USSOCOM. Initial Operational Test and Evaluation will be conducted as soon as practical, after Developmental Test is complete. The support we have received from the Department for an additional test aircraft will significantly reduce the technical and schedule risk for this "flagship" program. USSOCOM will continue to fund the procurement of SOF peculiar systems for the CV-22 such as the terrain following/terrain avoidance radar, and electronic and infrared warfare suites.

The FY04 AC-130U Gunship program continues modification of four additional C-130H's into the gunship inventory. C-130 modification programs provide for numerous survivability and capability modifications to our C-130 fleet. The Department accelerated the MC-130H Combat Talon II aerial refueling modifications to FY04 because this capability is crucial to the war on terrorism. In addition, the Air Force is providing USSOCOM 10 additional C-130Hs to convert to MC-130Hs. This increased capability will make up for attrition losses, enable SOF to forward-station additional rapid mobility assets, and allow us to assure our allies through increased forward presence. In FY04, we will continue programs including the Directed Infrared Counter Measure (DIRCM) Laser and several modifications to our COMMANDO SOLO fleet.

The Advanced SEAL Delivery System (ASDS) is a specially designed combatant submarine that will provide clandestine undersea mobility for SOF personnel and their mission support equipment. The ASDS is capable of operating in a wide range of threat environments and environmental extremes, providing increased range, payload, communications, loiter capability and protection of SOF personnel from the elements during transit. The ASDS provides a quantum leap in our undersea mobility capability. ASDS boat #1's Initial Operational Capability is planned for third-quarter, FY03. In FY04, program activities for the ASDS will continue to focus on procurement of long lead material items to support ASDS boat #2 fabrications and the development of technology improvements in the areas of sensors, cameras and communications. The ASDS is the only capability of its kind in the world.

In addition to the ASDS, USSOCOM remains committed to the Navy's SSGN program, converting four OHIO Class Ballistic Missile Submarines into dual role Strike/SOF platforms that will provide SOF with unprecedented worldwide access for both the ASDS and the SEAL Delivery Vehicle. The transformational changes incorporated into the SSGN will allow SOF to deploy a larger and more flexible force package than has ever been possible. Additionally, the

command, control and communications capabilities designed into these platforms will permit SOF to operate independent from, or in conjunction with, any land or sea-based Joint Task Force.

***Research, Development, Test and Evaluation (RDT&E)***

USSOCOM must continue to invest in making our SOF more capable in all environments. Our Research and Development (R&D) activities focus on exploiting technologies to improve SOF Command, Control, Communications, Computers, and Intelligence (C4I), mobility, weapons, and survivability. Our R&D program, while modest, is producing great capability enhancement products. USSOCOM's FY04 RDT&E request is \$440.4 million, as compared to \$512.5 million in FY03.

Two examples of capability enhancement products are our National Systems Support to SOF and our Advanced Tactical Laser (ATL) Advanced Concept Technology Demonstration programs.

The National Systems Support to SOF project is successfully integrating national intelligence systems capabilities into the SOF force structure. For example, the project is rapidly transitioning Blue Force Tracking equipment from development to operational use by SOF deployed in OPERATION ENDURING FREEDOM. These systems enable command and control elements, as well as combat search and rescue elements, to identify and track friendly forces. They also significantly increase our capability to execute surgical strike missions in the proximity of friendly forces by providing an effective means to distinguish between friendly and enemy forces.

The Advanced Tactical Laser (ATL) ACTD evaluates the military utility of a tactical directed energy weapon on the battlefield to provide support to the war fighter. A directed energy weapon has inherent performance capabilities that can support extremely precise and selectable strikes, effects and lethality, and multi-axis engagements. In FY04 program activities will focus on design completion of an objective ATL system,

procurement of long lead material items, and begin the Military Utility Assessment (MUA) using ATL simulations and component hardware testing in conjunction with military exercises.

We are working on an array of improvements across our mission areas, including: improved body armor and chemical protection, advances in gunship armaments, developing and leveraging Information Operations (IO) tools. USSOCOM's primary success has always been ensuring we select the right people and train them for innovation: we equip the warrior, not man the equipment. We clearly recognize that the modern battlefield is comprised of land, air, sea, space and the virtual domains. IO has the potential to help SOF operators remain undetectable in hostile area -- a critical element in most SOF missions. We intend to actively pursue IO capabilities and develop standing authority to employ these capabilities when needed. This will improve SOF effectiveness and access to previously denied environments, and dissuade potential competitors from engaging even if they perceive quantitative advantage.

Some of our most successful development programs have or will make a real difference in the fight against terrorism. The Multi-Band Intra-Team Radio (MBITR) radio provides a small, lightweight, software reprogrammable handheld radio capable of providing both secure and clear voice and data communications over 100 selectable channels. Thanks to support from the Department and Congress, USSOCOM has been able to accelerate fielding of these radios to our forces.

Another program worthy of mention is the hemostatic bandage. The development and rapid fielding of the hemostatic dressing embodies the first of our SOF truths - that humans are more important than hardware. The family of hemostatic dressings, which include the fibrin and chitosen dressings, were not due for fielding until 2007, but with the heroic actions and ultimate sacrifices of SOF in Afghanistan, USSOCOM focused on accelerated

fielding of these dressings. Thanks to the combined efforts of the Department, the Services, and other Combatant Commands, this revolutionary medical technology was catapulted from the research laboratory to the field five years ahead of schedule. These dressings stop the bleeding almost effectively as surgical closure of a wound. We aim to put this technology into the hands of every soldier, hoping to end preventable hemorrhage on the battlefield.

#### **Military Construction**

USSOCOM's military construction efforts ensure our highly specialized SOF personnel and equipment are provided a modern array of SOF training, maintenance, operational, and command and control facilities to successfully execute SOF missions. USSOCOM relies on the Services to provide community support facilities and programs construction only for facilities directly contributing to SOF training, readiness and operational capabilities. USSOCOM's FY04 MILCON request is \$99.4 million for 12 projects.

#### **CONCLUSION**

Now and in the future, SOF continue to improve their ability to execute the war on terrorism, while remaining ready to deal equally with demands of both our warfighting and peacetime roles. SOF will be deliberate in its transformation to ensure continued support to critical national requirements. But let us never forget those who have paid the last full measure. We want to acknowledge the men and women killed in direct support of our Nation's response to terrorists since October 2001 and others lost or wounded in combat operations to ensure their skills were honed and ready for the next fight. We face adversaries who would destroy our way of life. In response, SOF will not rest until we have achieved victory in the war on terrorism.

Thank you for your interest in and continued support of our Soldiers, Sailors, Airmen, Marines, and civilians; the men and women of the United States Special Operations Command.





**FISCAL YEAR 2004 NATIONAL DEFENSE AUTHORIZATION ACT—DEPARTMENT OF DEFENSE'S INFORMATION TECHNOLOGY PROGRAMS AND POLICIES**

---

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON ARMED SERVICES,  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES  
SUBCOMMITTEE,  
*Washington, DC, Thursday, April 3, 2003.*

The panel met, pursuant to call, at 3 p.m. in room 2212, Rayburn House Office Building, Hon. Jim Saxton (chairman of the subcommittee) presiding.

**OPENING STATEMENT OF HON. JIM SAXTON, A REPRESENTATIVE FROM NEW JERSEY, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. SAXTON. Good afternoon. The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this afternoon to consider the Defense Department's information technologies policy and programs for fiscal year 2004.

The Department of Defense (DOD) annually invests billions of dollars in information technology, IT, to support its business operations and plans to invest similar amounts in fiscal years 2003 and 2004. The defense IT budget request for fiscal year 2004 is approximately \$28 billion. This is a sizeable amount of funding for IT programs, systems and services that needs to be properly managed at both the Department of Defense Chief of Information Officer Department and the Service Chief Information Officer levels.

Technology changes evolve rapidly, and its integration is equally complex, thereby raising concerns that if IT programs and investments are not wisely planned with sound best business practices, coupled with an investment strategy, they are doomed to fail and cost billions and billions of dollars. This is a critical issue for DOD because its past investments have met with only limited success.

The subcommittee is concerned that one reason for this lack of success may be attributed to the fact that DOD does not have the corporate blueprint or enterprise architecture to guide and constrain its IT investments in a manner that promotes interoperability and minimizes duplication and overlap.

DOD is now developing a Department-wide enterprise architecture that encompasses seven functional areas: One accounting; two, collection of accounts receivable and cash management; three, financial and management reporting; four, human capital management; five, logistics; six, procurement, payables, acquisition and disbursement; and, seven, strategic planning and budgeting. The subcommittee is interested to learn from the witnesses what

progress the Department and the individual services have made in regards to each of these functional areas.

Secretary of Defense Donald Rumsfeld has stated on multiple occasions that IT is an enabler behind defense transformation. What is needed today is the ability to leverage the technology to ensure its operable capacity in both business and warfighting environments.

While the subcommittee recognizes the critical efforts and difficulty of IT modernization, concerns have been raised that there is not sufficient oversight at the Department nor at the service Chief Information Officer (CIO) levels to achieve the objectives contained in the Department's enterprise architecture. The General Accounting Office (GAO) has recommended that the Department develop an enterprise architecture in the investment management controls for effectively implementing the architecture.

GAO recommends that DOD should limit its IT investments to, one, deployment of systems that involve no additional development or acquisition costs; second, stay in business maintenance needed to keep existing systems operational; third, management controls needed to effectively invest in modernization systems; and, four, new systems or existing system changes that are congressionally directed or are relatively small, cost-efficient and low risk.

The subcommittee is interested to learn more about how DOD and the service CIOs are managing their IT plans, programs and processes and if the enterprise architecture is broad enough to give the Department and service CIOs the authority to effectively oversee both DOD's corporate transformation and DOD's force transformation command and control. This hearing will attempt to determine how successful are the Department and the services at modernizing its IT business systems and to effectively and efficiently—and how efficiently it is delivering the necessary IT tools and systems to the warfighters.

Let me just at this point yield to Mr. Meehan for any remarks that he might wish to make, and then we will introduce our panelists.

[The prepared statement of Mr. Saxton can be found in the Appendix on page 415.]

**STATEMENT OF HON. MARTIN T. MEEHAN, A REPRESENTATIVE FROM MASSACHUSETTS, RANKING MEMBER, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. MEEHAN. Thank you very much, Mr. Chairman. I want to associate myself with your opening comments, and I join you in welcoming our guests and I thank you for calling this hearing.

As you know, Mr. Chairman, I view information technology, or IT, as critical to both national security and economic strength of the United States. It is, in the words of Defense Secretary Rumsfeld, a true enabler of defense transformation. Indeed, it holds the promise of consistent global time-critical targeting. With the national security establishment growing increasingly reliant upon commercially available information systems, the Department of Defense IT modernization pushes the private sector to stay at the

forefront of technology development, just as our defense establishment endeavors to ensure stable economic markets abroad.

Not all is rosy, however. Many of the existing Department of Defense IT systems remain redundant and outdated; some are inefficient; and many are vulnerable to cyberattacks from terrorists, transnational criminals and even foreign intelligence services.

To guard against such attacks, we must successfully initiate both corporate and force transformation in the Department, even if suggested, as GAO historical assessments, that DOD's most important development projects often experience cost overruns, take longer to produce and deliver less than promised.

Just this week the General Accounting Office delivered more bad news. The DOD financial management system remains inefficient and vulnerable to fraud, waste and abuse, but we have little choice other than to modernize. IT products and services have become essential to the Department of Defense operations and battle plans. The solution must include a commitment to invest, reorganize and, finally, to empower those in need of information. I am hopeful that we can be successful but recognize it will take time, patience and considerable resources.

Just as I am encouraged by Department proposals, I am also realistic about the daunting task we face. I look forward to working with the Department and also with my colleagues on this subcommittee and my colleagues on the full Armed Services Committee. Thank you, Mr. Chairman.

Mr. SAXTON. Thank you, Mr. Meehan.

Before we introduce our panel, let me welcome our special panelist, Congressman Howard Coble, who is chairman of the Judiciary Subcommittee on Crime, Terrorism and Homeland Security.

We have two panels of witnesses for our proceedings this afternoon. Let me welcome the Honorable John Stenbit, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C4I). As such, he speaks for the Department and advises the Secretary of Defense on these issues. Rear Admiral Nancy E. Brown, Deputy Director for Command, Control, Communications and Computer Systems on the Joint Staff; and Lieutenant General Harry Raduege, Director of Defense Information Systems.

At the outset, let me ask unanimous consent that your full statements be included in the record; and let me say that we are going to be looking to you over a long period of time for your help and guidance on these issues. They are issues that are being for the first time discussed in this context, and we look at it as a major responsibility inasmuch as nobody would call \$28 billion less than major, particularly in regard to these issues that help to make our lives easier but, more importantly, more efficient. So we look forward to your testimony.

Mr. SAXTON. You may proceed as you see fit, Mr. Secretary.

# **STATEMENT OF THE HON. JOHN STENBIT, ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE**

Secretary STENBIT. Thank you very much, Mr. Chairman.

I am going to lead off with a brief statement. You have my statement for the record. You actually have a summary of that, as if I would summarize it.

What I thought what I would try to do this afternoon is give you a couple of examples of what it is we are talking about to set an overall context, and then we will be happy to hear the statements from my colleagues as well as answer all of your questions.

First, hearing the opening statements, I think I need to make a comment about definitional terms. The term "business system" and the term "IT" and the term "national security" sometimes get confused in all of this. I am here to represent, as the CIO of the Department, all of the aspects of the IT community. That is the business systems as well as what we call the national security systems or those that have the warfighters actually able to do their job.

There is a big difference between those two kinds. For instance, one of you mentioned that the GAO recommended that we do not use any IT systems that don't have any R&D in them. I am sure by the time I finish giving my talk you will understand I can't do that, because we do have research and development that are required to put satellites in space, that put laser communications in space, that actually build an infrastructure for our battlefield to be able to be done more effectively. So we need to keep track of at least several subjects at the same time.

I am going to try and go over the entire issue, because, from my point of view, information flows in the Department. While it is easy to tell a targeting loop and it is easy to tell a paycheck, they actually go together because we need to know where that person is, we need to do their health care, we need to do their logistics for them. So from my point of view it is all an integrated system.

But, for the record, I believe the \$28 billion breaks out approximately one-third for business-oriented things. So the eight functional areas that you described are in the range of a third to a quarter of the \$28 billion, and the rest is what we refer to as the—what Congressman Meehan referred to as getting the warfighters to be able to use information effectively.

When the Secretary says IT, he is talking about the whole gambit. He is actually in his mind even talking about satellites. Because, to him, that is all information, and he is thinking about that as part of the transformation.

So with that introduction, just to make sure we understand we are covering the entire waterfront, although we are happy to talk about any of the details you might like, I thought it would be appropriate to talk about where we were, where we are and where we are going and see if I can use some analogies and tell you about why it is we think we are moving forward in the way we are going.

You are correct. We do need an end-to-end architecture and an end-to-end game plan that talks about how do we actually continue to fund what we are doing today and dependent on while we move forward. Because it is a difficult management task because we can't just sort of unplug the system at any point in time.

About 25 years ago, I actually had the same sort of job then, working for Mr. Rumsfeld, that I do today. I don't move very fast in my career, I guess. Actually, I am one door down the hall at the



Pentagon. We ran a system that fundamentally you could think of as a telephone system.

I would like to start today by thinking of a telephone system as a smart-smart-push system. If anybody found anything out, they had to be smart enough to know that it was important; and then they had to be smart enough to know to whom they should tell it to, because they needed to know the telephone number of who it was that might be interested in that.

There was a Congressman from West Virginia—his name was Mollohan—who had almost in continuous session an investigative subcommittee that looked at the failures of that particular system over and over and over again, basically because it was too slow and it was a fundamentally impossible information system to make work.

I will use as an example, when the North Koreans captured the Pueblo, it took them 30 hours to get the Pueblo from where they captured it back into the port. But because we had this telephone system where people were dealing with a subject they didn't understand and they weren't used to the phone numbers, weren't on the list of who to call, it took us 36 hours to figure out that the Marines had aircraft in Okinawa that could have gone and intercepted it. Well, that didn't do us any good because it was already back in port.

We had cases over and over and over. Those were fundamental to this idea that we were in a telephone world, a smart push that you had to know what was important and then a second smart that you had know to whom you sent it.

Today, we are not in that mode, absolutely not in that mode for a big reason. From an information standpoint, we now have a smart push system, but it is more like direct TV. What it is today is anybody who finds anything out still has to be smart and know that it is important. But today they put it on a broadcast system, and they don't know to whom it is going. It goes all over the world.

That is what you see in action in Iraq right now today. If you go out and examine the command and control systems that are around in the military Department, as Admiral Brown and I did in the Middle East in January, you will see very large elements that have a thousand people or so with big complex networks and lots of satellite dishes out in the backyard all listening to these broadcasts, pieces of data. So when NIMA has a picture they think it is important, it goes on the National Imagery and Mapping Agency (NIMA) broadcast. When National Security Agency (NSA) has something that is important, it goes on the NSA broadcast. When the Air Force has something in JSTARS, it goes in the Joint Surveillance Target Attack Radar System (JSTARS) broadcast.

So we have separated, if you wish, the requirement for somebody who finds something interesting to know who might be interested in it. That is a big, big difference. What it has done is to transform what used to be a—we were fixed in time, and we were fixed in space in the old telephone system. If somebody wanted to talk to somebody, it only worked if they were there at the same time. So we are fixed in time.

It also worked—only worked if you picked up the phone; and if you went too far away, your phone stayed where you were. So you

were sort of fixed in space as well. We may have been spread out, but we couldn't wiggle too much from our common ground.

Today, we are now open in where we go. We can go anywhere and receive these broadcasts. We are still stuck being fixed in time, because the picture only goes out once on the NIMA broadcast. You have to record it. You have to process it along with NSA data, along with the operational data, along with the JSTAR's data.

That is what these people are doing in these command centers and fusion centers around the world these days. They take all of these real-time data—if you think about watching all the NFL games simultaneously on Sunday and figure out what is the best tackle play while looking at all the channels at the same time, that is sort of what we have to do in our command and control system today.

But what that allows is the proverbial guy on the wooden saddle on the horse in Afghanistan to say, I want a bomb over there, put it in a broadcast, and a B-2 pilot who is coming from Missouri and has been in the plane for 16 hours puts the bomb at that particular place. They don't know each other. They didn't have to know each other. They didn't have to know the phone number. They just had to know, on the one hand, I want something there and, on the other hand, I got a bomb and I can get it there. That is how we are doing it today. An amazing transformation. It is a big, big deal.

However, this subcommittee is actually about terrorism and unconventional things and so forth and so on. The very heart and soul of those subjects is that we are going to spread even further out in geography and we are going to deal with smaller and smaller groups of people that can do nastier, nastier things as a function of time. So that means we not only have to be flexible in space as we are today, we have to make it cheaper to allow somebody to participate in this, rather than buying eight satellite dishes and a thousand terminals and having a big, complex system to record all of those data and figure out what they say.

In order to do that we need to go away from smart push and go to smart pull, and the comparison to that is the Internet where the person who has the job goes back and finds the data they need. They don't need big, complex computers. They don't need big, complex storage or satellite antennas. They need an access to the Internet.

So the transformation that we are doing within the Department, while at the very same time we are operating in this very dynamic broadcast system we have today, which I call smart pushes, is we are moving toward a smart pull system.

Now if you think about that, there are a couple of things that are important: One, more than one person might pull the same data at the same time. It might actually be quite interesting. I need more bandwidth. I need to be able to use communications efficiently in order to allow personal tailoring of the information.

Today, it is sort of like you can subscribe to any magazine or book, but you can't call up the authors. You get what they send you. How many times have we heard at the end of a review of something bad that happened, the information was available, it just wasn't at the right place at the right time? Well, that is a statement that says smart push wasn't quite smart enough that

day because they didn't think those pieces of data were important in the context.

Right now, today, if a satellite goes over Iraq, I assure you the pictures of Iraq go out first. But if I happen to be in Afghanistan and it is my job to go over the hill this afternoon, it doesn't do me any good if the picture comes tomorrow. That is this tyranny that we are fixed in time today, not fixed in space.

In the smart pull, I will be able to do that. I will be able to pull the picture, maybe not have the expert look at it, but I will be able to take it and do it on my time scale with my kind of criteria.

That is the big overview of what we have been doing. In my statement, I summarize some of the programs; and I will be happy to talk about that as we move forward. But I thought it would be appropriate to give you a sort of a bigger picture view of what it is we are trying to do and why.

I think I would go back and summarize and say we went from the telephone to the television, and we want to go to the Internet. We went from—we were locked in space and time. Today we are flexible in space but not in time, and we want to go to we are flexible in both time and space. That is the big, overriding move of virtually everything we are doing.

Hopefully, that was helpful.

Mr. SAXTON. Thank you very much. Great explanation.

[The prepared statement of Secretary Stenbit can be found in the Appendix on page 419.]

Mr. SAXTON. Admiral Brown.

**STATEMENT OF REAR ADM. NANCY BROWN, DEPUTY DIRECTOR FOR COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS (J6), JOINT STAFF**

Admiral BROWN. Thank you.

Mr. Chairman, members of the committee, I want to thank you for the opportunity to testify here today. Before I begin my remarks, I would like to thank all of you for the support that you provided to the men and women of the Department of Defense and the military services and especially at this critical time that we are facing. Your continued investments are key to our ability to complete current operations in Iraq and carry out the war on terrorism.

I would also like to offer Lieutenant General Kellogg's regrets, as prior commitments precluded his appearance here today.

My testimony will focus on the Chairman of the Joint Chiefs of Staff top priorities: winning the war on global terrorism, enhancing joint warfighting capabilities and transformation. I will emphasize how networking and connecting our existing systems in new and creative ways support the achievement of these priorities.

I will start by discussing an overarching concept that guides all our Command, Control, Communications, and Computer investments, commonly referred to as "net-centric operations."

Finally, I will share with you some of the important progress we have made in identify some of the challenges we still face.

The net-centric concept is based on the premise that a weapons system itself is not nearly as capable alone as it is when it is seamlessly linked to other platforms, all receiving the latest intel-

ligence and command and control information. It also assumes that the supporting communications links will allow timely exchange of information and enable commanders to synchronize all available sensors and weapon systems to dramatically increase combat power, a true transformation of military affairs.

The Global Information Grid (GIG) is the underlying infrastructure that provides the secure networking capabilities that make net-centric operations possible. Net-centric operations is not an exotic concept requiring decades of research and development. We can reasonably achieve a limited capability through the use of existing and emerging commercial off-the-shelf and military technology, including new wireless systems. However, more and more frequently we find ourselves in competition with the frequency spectrum, with the commercial sector. While we recognize the growing private demand for spectrum, our ability to operate continues to be threatened by the transfer of military spectrum to the commercial sector.

Over the past few years, we have expanded the capabilities of our command and control infrastructure, including significant expenditures on leasing commercial satellite capacity. While the commercial capability provides a valuable surge capacity, it is not a substitute for a military program. We must aggressively pursue new technologies as well as identifying, developing and then sustaining the proper mix of military and commercial satellite capabilities to ensure that we meet the operational requirements of our tactical and strategic users. We must make important strides toward solving the interoperability challenges of our legacy command and control communications and computer systems, while ensuring our future systems are born joint, including prioritizing critical information systems efforts in the development of a new streamlined capabilities base requirements system.

There is no shortage of challenges and opportunities in the information superiority arena. One of particular note is information assurance. Our increasing reliance on information resources and systems, combined with the growing number and sophistication of network attacks, underscores the need to protect our information. This requires development of the tools and techniques along with retaining the trained personnel to rapidly detect intrusion, determine the source and respond appropriately.

Finally, we must not use our C4ISR budgets as billpayers for other programs as we may risk the information superiority advantage that we have already gained.

In conclusion, I believe we are making solid progress toward implementing a joint strategy for information superiority that supports our warfighters.

Mr. Chairman and members of the committee, I look forward to helping make the information superiority strategies that I have shared with you this afternoon a reality and to addressing you in the future regarding our progress and the way ahead. Again, I would like to thank you for the opportunity to be here this afternoon and stand ready to answer any questions you may have. Thank you.

Mr. SAXTON. Thank you very much.



[The prepared statement of Admiral Brown can be found in the Appendix on page 429.]

Mr. SAXTON. Just for the benefit of members of the panel, General Raduege is going to use this set of slides that are in everyone's packet.

**STATEMENT OF LT. GEN. HARRY RADUEGE, DIRECTOR,  
DEFENSE INFORMATION SYSTEMS AGENCY**

General RADUEGE. Thank you very much, Mr. Chairman. It is a pleasure to appear before the subcommittee today and discuss the Defense Information Systems Agency (DISA), the combat support agency that supports our Nation's warfighters and other defense activities.

I am now going to go to page two of the charts I provided.

[The charts referred to can be found in the Appendix beginning on page 537.]

DISA plays a key role in the success of three quadrennial defense review goals we have underlined on the left side of this chart. This also performs an important part in enabling the other three goals. Shown on the right are DISA's five core mission areas, plus other best-fit mission responsibilities that we have been assigned.

Chart 3: To fulfill our responsibilities, DISA has people stationed worldwide supporting C4 systems that serve the very needs of the President and all of the Department of Defense.

Chart 4: DISA provides global communications primarily through commercial assets supplemented with military value-added features which are listed in the center of this chart. These military features are critical to ensure U.S. Forces are not denied access to information, geography or space. The Defense Information Systems Network, or DISN as we refer to it, carries the vast majority of DOD's communications. DISN is the linkage between every military fixed location and our Nation's deployed forces and provides classified and unclassified voice data, video and conferencing.

We also have several initiatives to increase DISN capability. The Global Information Grid Bandwidth Expansion allows us to provide that needed bandwidth that Mr. Stenbit noted earlier. This provides bandwidth to critical command centers and intelligence centers to benefit our Nation's warfighters.

Today I will also briefly discuss the DOD teleport program which I have listed on that chart. The DOD teleport program will improve deployed warfighters' access to the DISN by greatly expanding connectivity. In the past, deployed forces connected to the DISN on X band frequencies through military satellites. Now they will be able to also gain access through teleports to many commercial satellite frequencies. To meet combatant commanders' needs, we have accelerated DOD teleport fielding. The increased capabilities represented by DISN services are integral for a warfighter's success.

As examples, real-time operational pictures of the battlefield, Predator video and soldiers calling in air strikes from horseback, as Mr. Stenbit described, are all made possible through the DISN.

Chart 5: We have made tremendous strides in expanding the global DISN infrastructure and dealing with increased system usage. As you can see, in the U.S. Central Command area of operation alone, we have experienced tremendous increases in DISN



services. Interestingly, some of our greatest increases have occurred in mobile satellite telephone usage where warfighters can acquire DISN access anywhere and at any time. Since September 11, the number of users has increased by 300 percent, and usage has peaked at 2.5 million telephone minutes per month. Additionally, fixed commercial satellite communications usage has increased by approximately 800 percent.

Chart 6: It is also important for commanders to have tools for joint command and control in order to understand where red and blue forces are located, to receive status on supplies and maintenance and to communicate via secure messaging. DISA's command and control systems provides commanders with these tools. DISA's Global Command and Control System, referred to as GCCS, provides information to decision-makers.

GCCS has been essential to Operations Enduring Freedom and Iraqi Freedom. Real-time data feeds are providing situational awareness of the air, land and sea battle space, complete with the accelerated fielding of key intelligence enhancements that have significantly improved sensor-to-shooter coordination.

Today, GCCS is the system responsible for providing Predator unmanned aerial vehicle (UAV) feeds directly to our pilots who are delivering precision-guided munitions onto the most critical enemy targets.

Commanders also require accurate information on combat support functions such as logistics and maintenance. This Global Combat Support System, referred to as GCSS, is currently providing this accurate information picture in seven combatant commands. GCSS is credited with reducing airlift information retrieval time from hours to minutes.

Unclassified and classified messaging is handled by the Defense Message System, referred to as DMS, and is derived from commercial products with military enhancements to ensure delivery, message integrity, authentication, security and positive identification of recipients. Today, DMS is operational at 270 military installations and is on schedule to allow us to shut down the 41-year-old automated digital network in September of this year.

Chart 7: DISA provides several key capabilities to achieve interoperability among U.S. And coalition forces. We try to ensure that interoperability is built in from the beginning as systems are developed and maintained through their life cycle. Our interoperability efforts include establishing DOD standards, information exchange, testing and certification, on-site support for operations and exercises, and spectrum management. These capabilities are delivered through DISA's joint interoperability test command, defense spectrum office and joint spectrum center.

Chart 8: Defensive information operations permeates every aspect of our organization from physical security to developing, fielding and operating all DISA systems. Our most responsive and flexible initiatives are the Global Network Operations and Security Center, referred to as GNOSC, and the DOD Computer Emergency Response Team, referred to as the DOD CERT.

The DISA GNOSC is the single DOD network operations center with a complete view of the secure and nonsecure global networks of the DISN. The GNOSC controls actions across the DISN to pro-

tect and manage DOD communications. Once the GNOSC identifies a suspicious event, the DOD CERT then takes over and analyzes it to determine the appropriate response. The GNOSC and the DOD CERT then provide direct support to U.S. Strategic Commands Joint Task Force for Computer Network Operations, also referred to as JTF-CNO. This is DOD's lead organization for computer network defense and attack operations.

As shown in this picture, the GNOSC, DOD CERT and JTF-CNO are co-located to achieve the synergy required to defend DOD information networks. During calendar year 2002 they detected, analyzed and responded to more than 46,000 intrusion events on DOD's nonsecure networks.

Chart 9: This also provides secure and nonsecure mainframe and server computer operations for more than 700,000 users and 1,200 applications. Our facilities have been designed to provide a secure, available, protected, disciplined and interoperable environment that is under military control.

Figure 10: Over the past 11 years, DISA has reduced the number of computer processing sites by 97 percent and decreased government manning by 90 percent, billing rates by 80 percent and operating costs by 70 percent. This occurred despite a 60 percent increase in mainframe workload. The latest customer survey conducted by the Gartner group showed that customer satisfaction ranked significantly higher than the average for commercial service providers.

Chart 11: In addition to our DISA core missions we have responsibilities for some other very important missions. Specifically, our White House Communications Agency supports the President, Vice President and other executive members with communications. Our Defense Technical Information Center hosts more than 100 DOD Web sites and is a clearinghouse of scientific and technical information to support DOD research. DISA's E-business Applications Division supports electronic commerce with on-line solicitation, paperless contracting and bill paying. Finally, our Enterprise Acquisition Service provides contract vehicles to DOD and nonDOD activities to support every telecommunications need.

The last chart: DISA exists as a combat support agency to provide C4 capabilities for our Nation's warfighters and Defense Department.

I want to thank you, Mr. Chairman and members, for this opportunity to appear before you today; and I welcome your questions.

[The prepared statement of General Raduege can be found in the Appendix on page 452.]

Mr. SAXTON. Well, thank you very much for three really outstanding sets of testimony.

As I was listening to all of you, it reminded me of a time in 1985 right after I had been elected to Congress. I went out to Fort Dix, which is in my district; and the military folks there started with a set of acronyms that I was unfamiliar with. As I listen to your testimony, I see I have some more learning to do.

General RADUEGE. I tried my best, sir.

Mr. SAXTON. We thank you.

Something I learned wearing another hat here in Congress you have reinforced today. As the chairman in the last session of the

Joint Economic Committee, we set out to determine what it was that was different about the conditions that permitted almost 20 years of continuous economic growth that took place during the 1980's and 1990's. We looked at government activities, and we saw maybe tax policy had something to do with it, maybe monetary policy had something to do with it, maybe spending policy may have had something to do with it, maybe promotion of international trade had something to do with it.

After we looked at all of those things, all of a sudden we got a new staff member that said, you don't understand how productive technology has made the American worker. And the charts you have showed us, particularly the charts on slide 11—the four charts that appear on slide number 11 go to reinforce that very concept.

So we thank you for those presentations; and I can certainly relate to it, having studied the benefits of technology from the other perspective.

Mr. Meehan, would you like to lead off?

Mr. MEEHAN. Sure, thank you, Mr. Chairman.

Mr. Secretary, I was amused with your analogy about the IT challenges and responsibilities. It is like watching an NFL game on Sunday and determining where the best tackle play was on a given Sunday. Being an NFL fan makes me wonder if perhaps the DOD should have hired Parcells instead of the Cowboys.

What is the status of the enterprise architecture and the investment management controls needed to implement it, and when will DOD have a plan in place?

Secretary STENBIT. We have a set of policies and procedures in place today which I use in my CIO function to determine the programs are in fact meeting the criteria that are both embodied in Clinger-Cohen and those that we wanted to use for our own management purposes and so forth. I can say that it is a first try, I think is the way I would look at it.

When I try to bridge both the three types of systems we have, we still have circuit-based, point-to-point communication systems where we need to deal with detailed interoperability argument. As I said, we rely today on the broadcast environment; and we are moving toward the net-centric environment.

The standards against which we measure existing systems and future systems started out rather broad. They are narrowing down dramatically as we speak because we are now investing in this very hard core infrastructure upgrade that I described—there are lots of parts to it, but, fundamentally, if we don't get the bandwidth higher, we won't be able to go to smart push. Once we do that, there are going to be a lot of people that are going to be a lot more concerned whether they can sell things to the Department of Defense if they don't match. So I think I can say we have the processes in place.

We had a review this morning of a very large personnel business system that has had some troubles in the past and has exactly the same kind of troubles, which is there is a past set of systems, a new one. Are they moving in a direction that is coherent, first of all, with respect to just their own little view? But then are they

moving in the direction that we are going to make for them when they finally finish their program?

So, yes, we have such a program. It is embodied by reference in the 5,000 series—8,000 series for information assurance. I forget, actually, the number of the procedures, but they are there, and people actually do respect it.

We are going to move with the GIG Bandwidth Expansion program. That is a program we have asked you for about \$500 million in 2003, which you most graciously gave almost all of it to us and an almost like amount next year—it is less, but same order of magnitude—to facilitate about 90 fixed installations around the world that are the heart and soul of either the intelligence or the command and control aspects of our Defense Department.

We intend to put one color of laser light via a fiber-optic to every one of those places. So when you saw General Raduege's chart that he is going from a couple of megabits a second to hundreds of megabits a second, we are talking—one color is 10 gigabits a second. So that is a factor of a thousand more than 10 megabits a second, which is equivalent to about three or four TV sets. So we are trying to jump-start the problem, get a lot of bandwidth there.

Once we do that, the end-to-end connectivity has to meet a much more rigorous requirement for standardization in the future than we have allowed in the past. No question about that.

There is a similar program called the Joint Tactical Radio System, which is a move to take what are today basically lots of radio programs that are done in the old acquisition mode of R&D, procurement, deployment, modification. We then attempt to make them interoperable. That is one of Nancy's big jobs. And we are going to do it with software control radios. But we have to establish a standard for those software controls, and then we will be able to have interoperable radios in the future. So we are moving toward a much tighter set of standards.

Mr. MEEHAN. Secretary Stenbit, I would like to raise an issue that deals with the upcoming Base Realignment and Closure (BRAC) round in 2005. I don't believe you have direct responsibility for developing BRAC evaluation processes or for executing the evaluation. Your area is relevant to the last active duty base we have in Massachusetts, Hanscom Air Force base, the home of the Electronic System Center (ESC).

You understand, Mr. Secretary, better than anyone just what role the ESC plays in C4I acquisition management and the value of those resulting systems to the warfighter; and I think you also understand better than anyone how important it will be for the Department of Defense to continue to have access to our Nation's greatest technological capability.

My concern is that those who are now determining the BRAC categories and evaluation criteria also understand these facts and work them into the process. As you may know, the past BRACs did not do that. Past BRACs were very good at adding up real estate totals and excess building space or evaluating the ability of training ranges. These criteria have only a passing relevance to the creation of an effective joint C4I system.

The last BRAC, for example, Hanscom Air Force base was actually evaluated by the length of its runway. It doesn't have a run-



way and doesn't have airplanes. What it does have is access to world-class technology and high-tech industry and academic institutions around it, labs, Federally Funded Research and Development Centers (FFRDCs). The programs that any of the services—product centers, if they are moved, it seems to me the disruption of program management, the programs that you oversee, could be significant and the disruption will cost money. It seems to me that this risk to programs is another crucial factor that has not found its way into the whole BRAC evaluation process.

So that the way I see it, creating a successful joint C4I management organization will entail all of the expertise and careful consideration that any large high-tech company would employ if it were embarking on a major reorganization. They would bring in their best technical minds and foremost management experts and best human resources people. The facilities and real estate people would be included, but they wouldn't run the effort.

So my concern is that we don't have the situation that we had in past BRACs so that the real estate people basically don't run the effort. I fear that the result if that same approach would be applied, that the C4I product centers would be victimized under such a process. So I am wondering how or if you would recommend to the Secretary that he adopt or adapt this BRAC process to optimize the joint C4I management capability; and if the Department were to shut down or move organizations in this procedure, what the effect would be.

Secretary STENBIT. I agree with several things you said. One, I don't think I have anything to do with it; two, Hanscomb contributes mightily to the solutions to the problems that I am interested in; and, three, there are switching costs in any large organizational move.

My view of the way the current Department works, which is all that I can refer to, is the Secretary has what is called the Senior Level Review Group. It is a SLRG. I don't like being called a SLRG, but we all are—all the direct reports including myself are on that committee, and we discuss the serious issues of the Department.

I think that is all I can say. I would be surprised if any other process doesn't follow the normal process where we all get to make sure that our points of view are taken.

Mr. MEEHAN. I just think it is important when you look at technology that intellectual and technical capital play a role here and that these facilities and labs aren't evaluated based on the length of their runway.

Secretary STENBIT. I recognize switching costs, and if they move one of the places that I am going to put one of these new fibers I have got to put it someplace else. That is a switching cost. There are lots of them.

Mr. MEEHAN. Thank you, Mr. Chairman.

Mr. SAXTON. Mr. Wilson.

Mr. WILSON. Thank you, Mr. Chairman.

Secretary Stenbit, I am impressed that you have been in this field 25 years.

Secretary STENBIT. Doing the same thing.



Mr. WILSON. Well, no, it isn't the same thing. That is, what is so amazing to me, the versatility that you have. I feel like you have come from the era of Alexander Graham Bell to the era of Mike O'Dell.

Mr. MEEHAN. He is not that senior.

Mr. WILSON. It just seems this way. But I am really impressed.

You also identified my major concern and that is the information being available but not the right place at the right time. Do you feel that we are making the right strides to achieve the goal that the information get to the right place at the right time?

Secretary STENBIT. There is no question that today we are much better at distributing important information more broadly than just a precise definition of exactly who needs it, and that comes from this broadcast system that I was describing. That has helped an enormous amount to allow people to get the data and use it in different ways based on the data.

As I said, it is a bit like being able to subscribe to any magazine you like, but you can't go to the library. So the answer is we are still dependent on the institutions that determine what is important to select the information which is said.

We have some experiments—we have a notable experiment here locally which we started last year, if I may say—in anticipation of that question—which we call the night fist exploitation facility. It is built to be a model of what life would be like if we had all the bandwidth that I was talking about and we could interactively talk with the data sources, as opposed to take what they give us and analyze what we get. We have a subset of that with the folks in Tampa. Both of those have come up with really very, very startling results.

For instance, if you were are to compare 1991 in Iraq and today in Iraq—and this is an unclassified hearing, is that correct—we were not very good at closing the time loop when a Scud would be shot; and if we could go over and try and shoot the tail after they shot it, we have been very good at that. This time, almost the reverse. We have had as many hits as we had misses and many misses as we had hits.

Mr. WILSON. It is like eight out of ten.

Secretary STENBIT. I am not going to go there, but you are right. It was closer to one out of ten last time, and closer to nine out of ten this time. And Night Fist has been part of that because it is a highly interactive, very specialized focus, as opposed to a global distribution of information where people piece together what is best. So we have some experimental data that says once we get to a total smart pool network, we will do a lot better than we are today.

Mr. WILSON. For all three of you, as we all enter into an era of wireless technology and the concerns that we have about security in a wireless world, what were your concerns and then what precautions or protections have been made to protect security?

Secretary STENBIT. Let me start with that. That is a touchy issue. People like their cell phones and their Blackberry, and those are very dangerous devices for more than just the data you put into them, and I am not going to go into that while we are in an unclassified environment. But just the existence of those without some-

body putting data into them are dangerous for the security of people around. So we have imposed a policy within the Pentagon about who can use what kind of devices where. It has caused all the screams, and people are objecting and all the rest of that stuff, but we had to do that in order to protect the security. So we are paying attention to that.

That is what General Raduege has to deal with, and that is what Admiral Brown has to do. Because in the networks it is the weakest points that count and not the strongest. But I need to get my colleagues who are doing it in an operational level other than the policy that I put out to discuss what you just asked.

Admiral BROWN. I do think that the policy is important, and it has given us some guidelines, but we also have to be able to take advantage of the technology that is available to us. So we have to work very closely with the commercial industry to help us resolve the security risks that those devices present and get them to help us come up with the security that will allow us to take advantage of that technology. That is what we are trying to do, and trying to stay ahead of that is very difficult in mitigating the risk at the same time.

General RADUEGE. I would just add it really comes down to the risk involved and what you are willing to accept. I know that I always think of my Blackberry that I used to have, which was—it has been taken away from me now. I do have a Cryptoberry now that allows some protection. But I always felt that those and any wireless telephone that I had, my cellular phone, anything that I said on that should be able to be posted on the front page of the Washington Post the next day. So it is a complement to the way you conduct your normal business, but you need to remember what you are speaking over and how it is going into the air.

Now for our warfighters today I will say we do have wireless capabilities, satellite systems and telephones that they use in Iraq and in Afghanistan that are secured. There is no probability or there is low probability of ever the people using them being detected, which, as you know, we turn that around on other people who transmit in the clear. But we have systems that we have given to our warfighters today, and they are being used very effectively. That is where we cannot accept risk or, if there is, it is very minimal.

We are also, as I mentioned in my brief statement in the beginning, we work the White House communications for the President. There his activities quite often in certain settings are very perishable information where we could use wireless capabilities to move him quickly. But after someone would detect it, he is already gone. So we are carefully using that type of technology in that setting.

So there are varying degrees of very secure versus acceptable risks and even complementary capabilities for the way we use and pass information over wireless systems. But certainly we look to industry to help us in each one of those regards.

Mr. WILSON. Thank you.

Mr. SAXTON. Thank you very much.

Mr. Kline.

Mr. KLINE. Thank you, Mr. Chairman; and thank you very much, gentleman and lady, for being here today. I have got a couple of questions.

It seems through a number of years of my service in an earlier life I must have attended hundreds, probably, of exercises of one kind or another; and I can't ever remember a report where we didn't report that everything went great except for calm. I suspect there is still some of that out there now. In fact, I was just looking at a magazine article, I think in Jane's, that was talking about some complaints that the Marines had with some interoperability; and I have been listening with great interest and great optimism and hope that we are going to move to a case where we can speak to each other in a common language over somewhat common equipment.

But two questions: That is, the plan—and Admiral Brown is working very hard making sure that is interoperable, but where are we right now in that ability to communicate back and forth? And if we are not there—and I just suspect that we are not quite there yet, based on your earlier testimony—when will we be there so we are, in fact, talking together over secure net?

Secretary STENBIT. You will find the report on what is going on in Iraq that we have a lot of confidence, and it is working very well. And I hesitate to say that on the record in front of the kind ladies over here, but it is going to be in the following context.

But it is going to be, in the following context that I described, a very robust, broadcast-based system, satellite-based, fiber-based. It is working extremely well in the large complexes that have the money to build the little tent cities and all the satellite dishes in the back. We have a lot better ability to tie those together today with the forces, because those forces are also in a lower bandwidth sense, feeding information so that there is a lot better two-way communications.

Is it good? No. I mean, is it—I think it is good. It is not perfect. What won't happen in the future is, if we don't spend as many months as we did this time—and we didn't set up all of these places, and it took us months to do it, and yet all the commercial communications—General Raduege and I worked the problem on the 12th of September, getting satellites up; it was a very exciting day.

So we are an awful lot better than we ever were before.

I am not too worried about going on the record that people will say it is really good. Now we have to be able to do it for those people that were in the convoy that went the wrong way on the bridge.

Mr. KLINE. Exactly. My concern is not so much that one headquarters cannot talk to another one, and probably secure; I am more concerned about the soldier/Marine that is out driving along in a Humvee or in a helicopter, as I was, and trying to get everyone in sync and go secure and not secure and all that.

Secretary STENBIT. You would be surprised.

Admiral BROWN. I do think you would be surprised. We are not there yet. But I think this year we made more progress under addressing our legacy systems and making them interoperable and planning that and getting the money in the budget to do those things that you mentioned than we have made in the past 10

years. We actually got new money, over \$2 billion put in the budget for specifically that item. And we will be able to, by 2008, we believe, have true interoperability, not just in our new systems that we are making sure they are both joint, but in our legacy systems that we still have.

Mr. KLINE. That is excellent. I am, of course, concerned about the legacy systems, because that is what we are using and 2008 doesn't sound like there is still time for that.

Admiral BROWN. But we have a good, solid plan. We have prioritized our systems so that those critical tactical systems are going to be the first ones addressed. That will be long before 2008.

Mr. KLINE. Okay. Thank you very much.

I see we are getting paged all over the place to go vote.

I have another question which I will just throw out. There has been some discussion about troops in the theater about being able to phone home one way or another. Is that bringing in a commercial system, or can you just very briefly answer that before we all spring up here and go run across the street?

Admiral BROWN. We are attempting to make sure that they can do that with phone cards, the capabilities are there, and it is just a matter of working out the details. I brag on my own service because the Navy has done that with cellular phones for a long time. It is a quality-of-life issue.

We are very concerned about it; and I think that we have a solution, and we are working toward implementing it.

Secretary STENBIT. Once again, in a broadcast system we are sending more than we are building the ability to come back. We need to go both ways. There is no question about that.

Mr. KLINE. Thank you.

Mr. SAXTON. Just two pieces of information. This little baby just told us that we have taken Baghdad Airport. So that is cool. Second is that—

Secretary STENBIT. That means he is going to walk when he runs?

Mr. SAXTON. The second is that those bells that you just heard announced the vote on the Cunningham amendment, which is to remove a billion dollars from the supplemental appropriations bill which is aid to Turkey. So we will spend 5 minutes on Mr. Bartlett's time, and then we will go vote and we will hustle back.

Mr. BARTLETT. Thank you very much.

At 9/11, our communications capabilities were overwhelmed and we were limited in whom we could talk to. That, of course, is a challenge that you are trying to meet. There is a limited system supported, funded by the National Guard—so many acronyms—National Defense Fiber Optic Network (NDFON). Are you familiar with NDFON? This is set up in Oklahoma, and it is a dedicated fiberoptic system that is dedicated to the military so that we will not lose—we are not sharing capability with anybody else.

So it has advances and a security, it has advantages in accessibility. And my question is, do you know of it and why shouldn't we consider that approach as a competitor to the beginning approach that you are now taking?

Secretary STENBIT. Let's see. We need an enterprise-wide system that goes not only from fibers in the ground—and let me assure



you that the problem of sharing bandwidth was not the problem on 9/11. The problem was at the tails, at the cell phone end.

As a matter of fact, General Raduege just did it on any voice system. We have distributed cards, and we have a system that is available in the United States that overrides the busy signal in the voice switch system if you are on a regular phone. And that all works fine and that is not a problem.

The problem we had on 9/11 was a cell phone problem and that we have made a little bit of improvement and, in fact, are prepared to do more, but it actually turns out to be, these days, a homeland defense issue. However, it is much better for us to be able to use an enterprise, end-to-end system as opposed to having multiple, special purpose systems as long as we provide the capacity to make sure that people don't get thrown off because that is how we are going to go from the special purpose—from the system to the radio that somebody needs because they are out running around in the Humvee that Mr. Kline was talking about. And, in general, the guard kind of systems connect up their own sites, but won't do very much good for us in Iraq.

So it really is an end-to-end enterprise system that is needed. And if there is capacity in alternatives, we would be happy to use it. But it is very important that we can get end-to-end the whole way.

Mr. BARTLETT. Can you look at that and tell us why that is or is not a good idea? Clearly, it is not—it doesn't go overseas, but tell us, for that part of the system with which it is competitive, why it is or is not a good idea.

Second question is, it has been a long time since we were pushing the envelope. Your use of satellite phones, is that going to make them available at reasonable rates in the marketplace now? Because they are not now available at reasonable rates.

Secretary STENBIT. I don't think we have done enough to the general commercial marketplace to change the economics.

Mr. BARTLETT. It would be nice if your technology was good enough to change that.

Secretary STENBIT. We are applying fiberoptic technology that the commercial people use in our case.

Mr. BARTLETT. You are not doing that with satellite phones?

Secretary STENBIT. But we are using the same technology, that is, going to lasers to go to satellites.

Mr. BARTLETT. Last question. How much of your system will still be available to you after a robust Electromagnetic Pulse (EMP) lay-down?

Secretary STENBIT. You mean delivered by nuclear weapons?

Mr. BARTLETT. Yes, sir.

Secretary STENBIT. There are lots of problems with the existing system when faced with nuclear weapons. The most likely EMP-only attack, this is a high-altitude attack, when you try to spread the electrons over as large an area as possible, in general the military systems will be okay; but we have trouble with respect to our dependencies on some of the commercial systems.

Mr. BARTLETT. For instance, your space communications, you move about 7 percent of all of your space communications over your



own satellites; the rest, 93 percent, are moved over private-sector satellites which are the weakest, the softest link.

Secretary STENBIT. I think your number is a little low, but I will grant you that there is a lot of commercial.

Mr. BARTLETT. On your U.S. Military Communications Satellite Program (MILSTAR) satellites, which is the only really secure space that you have.

Secretary STENBIT. The Defense Satellite Communications System (DSCS) satellites are hardened to EMP. They have large bandwidth. The military satellites are hardened.

I take your point, which is, there are satellites that we use that are commercial that have large bandwidths that are not hardened to EMP blasts. That is correct. The magnitude of the problem that you described, I believe is overstated.

Mr. SAXTON. We are going to have to go. We need you to stay for a few more minutes.

[Recess.]

Mr. SAXTON. Thank you for waiting. I detected that maybe you have some other things.

Secretary STENBIT. No. I knew I had four colleagues that wanted to have their opportunity.

Mr. SAXTON. We are going to give them their opportunity. We talked—you started out, Mr. Secretary, by saying that about one-third of your responsibility, or IT responsibility, for lack of a better term, is business oriented, and the other two-thirds is warfighter technology oriented.

We have spent most of the time so far talking about the warfighter two-thirds, and I think that is good. And there are a lot of things we haven't talked about on that side that—I was sitting here; things pop into my mind like the great capability that we have to protect our fleets with AEGIS technology, which is great IT stuff. We will be able to reduce the number of people that it takes to man the next generation of warships, DDX, from whatever it is now—from 300, 400 to a little over 100 because of technologies.

My able friend, Tom, here and I were recently at Coronado and saw some unbelievable stuff that the SEALs are doing to help with certain functions with IT. Just this morning we saw—we had demonstrated by the Department of Defense the capability to know where all our forces are.

Secretary STENBIT. Full-force tracking, yes, sir.

Mr. SAXTON. Neat stuff, very valuable stuff.

You mentioned Patriot Advanced Capability-Phase 3 (PAC-3), and the successes we have had in countering international intercontinental ballistic missiles recently is also impressive. And that is cool.

I would like to talk about the other third for a minute. We need your help and advice in understanding how to evaluate what we do on the business side. The evaluation of—from our point of view, of what we do on the business side is less exciting than the things we have been talking about here, but obviously, from a fiscal point of view, just as important for positive reasons as well as for reasons that make it hard for us to understand.

I am not saying that there are things that we see that are questionable or anything like that; it is just hard for us to understand, when we are used to counting airplanes and buying bullets, and all of a sudden have to count computer capability. That is what we have to count; that is what you have to count, and you know more about it than we do.

So let me start with this question: How do we begin, as committee members who are not experts in this area—and we are trying to get some staff that is an expert in this area—how do we fulfill our oversight role with regard to that one-third of business-oriented technology in evaluating that capability—how much you need, how much we want to fund, and how to go forward in an intelligent way?

Secretary STENBIT. First, the one-third was the upper end of what I said. My instinct would have been to tell you, it is about \$5 million of the almost 30. But I didn't have the courage to because they threw a piece of paper down in front of me that didn't say that. So I will get you a better viewpoint if we can agree that there is a difference. That is really all I was trying to do as you rattled off eight functional areas.

In addition to that, those functional areas, we do the infrastructure that allows those functional areas to, after they develop their software and all the rest, to actually operate. General Raduege showed you part of the mainframe computer business and the communications that go with it. So it is a little difficult to pick which number.

Let's you and I agree that we are talking in the \$5 to \$8 million range for the business. And as we get to 8, we are getting pretty joint use, like logistics that is getting a lot closer to what the military forces use, and when we get to the 5 we are hard core paying somebody, or making sure they got their shots last week or something like that. It is in that range.

Now, actually, the government, the defense department as part of the management efficiency request that we are intending to put back over here, are actually making some suggestions that what we are told to do for Clinger-Cohen compliance on the business side has a lot of stuff that isn't particularly useful for either you or me.

So I think the dialogue you are suggesting, which is, how do you best get comfortable with how these programs are going and how do we best manage them, is a subject that should be of some interest to the Department. Because there is a lot of overhead reporting that is interesting, but not how you run programs, and I think that would be a place to start.

But in answer to your question directly, the reason that IT programs are difficult—and it is not unique to the Department or to the Government; it is true in large organizations as well—is because the people that own the processes, the finance people, the salespeople, the engineering people, it is their business process that needs to be changed that allows the investment in the automation to actually come to a positive result.

Just automating an old process has some utility, but it is not where the real leverage is. And it is this intersection that you were just describing, which is between the techie nerds like myself, who can figure out how to get software in computers and communica-

tions to work; but it is the intersection of that with the business process that the actual functional people use where the trouble comes.

And so my recommendation would be that you, as you look at the IT programs, you make sure the two things are going on: one, that the owner of the process is vitally and integrally interested in the program and has a handle on the requirements and has some process that doesn't allow just open-ended changes, because we have learned on the military side there is—the worst word in the world is, We can make that a little better; all we need is a software change, okay? And that is what causes programs to take longer and cost more and not work as well and all the rest.

In the IT business it is all software. And so the pressures that go on, the actual people that are doing the business process re-engineering, when some guy comes and buzzes in their ear they have this great idea, they have a tendency to succumb. And what you need to assure is that on the requirement side, the people that own the process have a vigorous way to understand how they do it today, how they are going to do it tomorrow, how they are going to train their people to go through the transformation.

And then you need to look to me and make sure that I am managing the actual implementation of the program that is, in general, described as the computers and the communications and the rest that happens.

Now, I am ultimately responsible for the Secretary, but I am not responsible for the finances of the Department; Dov Zakheim is. So when he is doing his financial modernization, I can review his program and make sure that he is meeting the Milestone requirements. But it is not my job to figure out, nor should it be my job to figure out, how he wants to conduct the accounting standards of the Department. When Pete Aldridge is doing the acquisition, or the manager of the Defense Logistics Agency, they have their priorities.

You asked me a question about how I would recommend that you do it. I would recommend that you look at both sides, that you pick whatever one you want to pick; you had eight areas, some of those have very good requirements processes.

I will share with you, at the expense of getting in trouble here, the medical community is very robust at how they are defining the requirements for their automation programs, how they reach out to the pharmacy—pharmaceutical industries to do integrated supply chain management so that they don't have to store all the drugs, that they are connected, as Wal-Mart is, to their suppliers, an unbelievably fine job of business process engineering. And there the issue of the money to be saved is so large that even if we overran the computers, it would be a good deal.

I am not suggesting we want to overrun the computers. But there are other cases.

Mr. SAXTON. What does "overrun the computers" mean?

Secretary STENBIT. We have a program that we think is going to take 24 months and it is going to cost \$8.6 million, and it costs \$12 million. That is what I meant by overrunning, doing a bad job of performance.

Mr. SAXTON. That is a—we often draw the comparison between what the Department of Defense may want to do when increasing technology and capability, and we often compare it to business. Well, if you are Mr. Wal-Mart, Mr. Wal-Mart has to say, Do I want to make this investment to gain these capabilities to make my company more profitable? So there is a built-in measure in the private sector which isn't necessarily built into the Department of Defense. Would you agree?

Secretary STENBIT. No. I think the pressure—I am basically from the private sector. I have been in the Government twice, but there is no question that I am not a government person and my colleagues will be happy to attest to that.

But the Clinger-Cohen process absolutely requires a cost-benefit analysis, a return on investment analysis, for every IT program that the deputy does or any other part of the Government does. The process is there to come up with the same kind of analysis that the Chief Finance Officer (CFO) at Wal-Mart would do about whether he should or shouldn't invest the money.

The problem is that that is done at the beginning of the program to get it going. But it is taking a look at the end of the program and the changes that occur as you go along; it is not as interactive as it would be at Wal-Mart. I think that is one of the problems.

But it is not true that return on investment and cost effectiveness are not used; it is just that the Government doesn't tend to do that in an iterative way; they tend to do that in a review way, and then the recovery paths are more difficult to handle.

So I wasn't trying to be obstreperous, but that is one of the things that I was worried about. If I come up to you with precision down to the \$100,000 level on a \$30 million job, which I don't know it is to that accuracy, because I haven't done the job yet—I would know it within \$5 million maybe—I have overdone the precision at the beginning and I have underdone the ability to change the authority as we move forward. But you have heard the complaint by lots of people who have talked about program elements before.

The key, though, is that we both collectively know that the requirements are under control and that the processes to make sure that they make sense and that the business process reengineering that makes the money gets saved is what is really important.

Mr. SAXTON. Well, thank you very much. We appreciate all three of you being here, Mr. Secretary and Admiral Brown and General Raduege. Thank you for what you are doing, and for the watchdog role that you play in making sure that we have the best capabilities that we can.

It has often been said, at least in the circles that I run in, that today's threat is such that they may have the element of surprise on their side, but we have got the element of technology on our side, and so far it is working out pretty good.

So thank you very much. We appreciate you being here. We look forward to working with you in the future.

Secretary STENBIT. We appreciate the opportunity to have you help us apply the technology as fast as we can. Thank you very much.

Mr. SAXTON. Our second panel this afternoon will provide an outline of the IT issues and challenges that lay ahead for the service



Chief Information Officers, CIOs. Our witnesses are Lieutenant General Peter CuvIELLO, Chief Information Officer, Department of the Army; John Gilligan, Chief Information Officer, Department of the Air Force; David Wennergren, Chief Information Officer, Department of the Navy, and Brigadier General John R. Thomas, Director of Command, Control, Communications, and Computers, Chief Information Officer for the Marine Corps.

Welcome aboard. We are glad to have you here to continue this dialogue this afternoon. We will let you proceed when you are ready, as you see fit.

Mr. SAXTON. General, I think you are probably first up.

**STATEMENT OF LT. GEN. PETER CUVIELLO, CHIEF  
INFORMATION OFFICER, DEPARTMENT OF THE ARMY**

General CUVIELLO. Thank you, Mr. Chairman. Mr. Chairman, members of the subcommittee, great to be here.

I am the CIO of the Army, but I am also the G-6 of the Army which is the operational arm within our Army. I am pleased to be here today to appear before you, and I want to share with you how the Army is leveraging information technology to transform into a network-centric, knowledge-based organization and an objective force that we are moving towards.

I would like to thank you also, as the others did, for your support in this year's fiscal year 2003 budget and your concerns regarding our C4, Command, Control, Communications, and Computers and our Information Technology capabilities and program supporting the Army both at war and in our day-to-day business.

What I will describe to you today is not just a vision; it is happening today, as exemplified in Southwest Asia and in our day-to-day operations. The Army is fundamentally changing the way we fight and creating a force more responsive to the strategic requirements of the Nation.

At the same time, the Army C4 and IT must also change for this transformed force. To quote a 107th congressional report directing action by department CIOs, "The committee believes that the overall interest of the Department of Defense and the Intelligence Community would be best served by quickly moving to a network-centric environment."

The Army has completely embarked on this, and the Department of Defense's network-centric warfare vision scene is making significant progress as we transform our systems platforms and processes to achieve the network-centric and interoperability in the Joint, Interagency, and Multinational environment as exemplified—as we are doing today.

The Army has consolidated management of information technologies into a single effort which we call Army Knowledge Management, AKM. The overall strategy is to improve information delivery to the warfighter while reducing overall costs. To that end, we are integrating best business practices; managing the information technology infrastructure as a single enterprise; providing Web-based, secure network access for the entire Army; and most importantly, harnessing our human capital.

This will enhance lethality on the ground and decision-making at all levels, supporting both the warfighters and the goal of the



President's management agenda to secure the best performance and the highest measures of accountability for the American people. The fundamental shift in culture and process has resulted in tremendous efficiencies and increased capabilities in the command and control arena; and we are aggressively applying the same processes to our business systems and accompanying infrastructure.

The Army Knowledge Management strategy firmly supports the information management requirements established by the Clinger-Cohen Act. The Secretary of the Army and the Army Chief of Staff have empowered the CIO G-6, me, to oversee the IT investments to ensure efficient utilization of resources. I now provide not only critical oversight through strategic direction, but also through enterprise investment strategy and performance-based management of all programs within the Army.

As a part of the global information grid, as we have talked about before, our Army knowledge enterprise strikes the Army's IT framework from posts, camps, stations, National Guard armories and Reserve centers to the deployed combat forces. We have established the Network Enterprise and Technology Command, NETCOM, that brings together network operations across all components of this single enterprise. As the single network operator and defender, NETCOM provides the information assurance that is critical to the Homeland Security and our combatant commanders.

Protecting essential C4 and the infrastructure from potential cyberterrorist threats, our Army Knowledge Online provides the enterprise portal to this protective network. We are over 1.3 million subscribers accessing increasingly vital information and online services. Our AKO provides collaboration of Web-based applications that ensure information sharing among the warfighters, our business stewards and even our family members.

The Army continues to leverage the full potential of the technological advantages of our Nation's industrial, science and technology communities. The objective force is being designed from the bottom up around a single, integrated Army Knowledge Enterprise within the larger global information grid. We have a number of programs that enhance situational awareness and understanding across the force. Advanced technologies include commercial off-the-shelf software systems that provide the foundation for a "factory to foxhole" continuum of operations necessary to support our future combat system and our objective force. These solutions support processes across the enterprise, providing timely, reliable and quality information and replace "stovepipe" legacy applications with an integrated system of systems.

Another example, which you referred to before, our Blue Force Tracking System, fielded now in Southwest Asia, allows real-time friendly unit and material tracking and situational awareness for our combatant commanders.

We are leading Army transformation through information technology. On all levels, from the individual to the strategic, we are aggressively transforming to a network-centric, knowledge-based objective force. But we still have much to accomplish. With your help we will attain our shared goals in this decade and meet the guidance of both the Office of the Secretary of Defense and Congress.

Thank you, Mr. Chairman and distinguished members of the committee, for allowing me to appear today. I look forward to answering your questions and comments.

Mr. SAXTON. Thank you very much.

[The prepared statement of General CuvIELLO can be found in the Appendix on page 472.]

Mr. SAXTON. Mr. WENNERGREN.

#### **STATEMENT OF DAVID WENNERGREN, CHIEF INFORMATION OFFICER, DEPARTMENT OF THE NAVY**

Mr. WENNERGREN. Good afternoon, Mr. Chairman and distinguished members of the subcommittee. Thank you for the opportunity to appear before you today.

It is a time of transformation, and as the Department of the Navy's Chief Information Officer, I have the honor to work across the Navy and Marine Corps team in harnessing the power of technology for our sailors, Marines and civilians.

Our Naval Power 21 vision sets the course for interoperable, network-centric operations that will link warriors, sensors, networks, command and control platforms, weapons and commanders into a networked, distributed force. We are creating a seamless enterprise network structure comprised of the Navy, Marine Corps Intranet, or NMCI, the Department's shore-based network, IT-21, for afloat forces and Marine Air-Ground Task Force Tactical Data Network as our contribution to the DOD vision of a trusted, dependable and ubiquitous network.

As we roll the NMCI, we are seeing the power of a single enterprise network improving access, interoperability and information security and the value of a performance-based contract and integrated service delivery team as demonstrated during the incredibly swift reconstitution effort for the Navy team after the tragic events of September 11th.

But an enterprise network alone is not enough, and so we are simultaneously transforming the way in which information is shared to truly achieve knowledge superiority through collaboration and communities at practice. Our E-government efforts and E-business operations office have successfully transformed labor-intensive paper processes into reengineered, Web-based solutions to improve both quality of service and to produce substantial efficiencies across the Department.

Now we are beginning development of the Navy-Marine Corps portal and enterprise portal structure that will secure our vision of a Web-enabled department, providing our sailors, Marines and civilians with access to the intellectual capital of the Navy-Marine Corps team.

Mr. WENNERGREN. I am also pleased to report that we are making significant progress in pursuing an enterprise approach to portfolio management of our information technology resources. We have identified functional area managers and assigned them the responsibility for managing processes and applications within their area of expertise, and they have used this authority to reduce the number of approved applications in the Department by almost 90 percent from 67,000 down to 7,000.

Security continues to be a top concern for us, and our information assurance efforts focus on a broad array of initiatives to ensure defense in depth strategy. We are benefiting not only from the significant security enhancements of Navy/Marine Corp Intranet (NMCI) but also from our use of public near digital certificates.

As the Chair of the DOD Smartcard Senior Coordinating Group, I also lead the DOD-wide rollout of the common access card. To date DOD has issued 2 million smartcards, with the Department of the Navy accounting for 900,000 of those cards. We leveraged industry best practices and standards to develop a solution that strengthens both our physical and cyber security efforts. Our critical infrastructure protection efforts focus on mission assurance. We have put into place an integrated vulnerability assessment process for our regions and we have fielded a groundbreaking self-assessment tool that allows our base commanders to have the capability to assess potential infrastructure vulnerabilities and then remediate them.

Maybe even more importantly, we have partnered with State and local governments and industry in areas like Virginia, San Diego and the Pacific Northwest to share analyses, to share lessons learned, and to share consequence management strategies to raise the bar of security for all of us. But ultimately it is our people, those brave sailors and Marines deployed far from home in harm's way, that are the heart and soul of our organization. What they know and how they translate that knowledge into action will define how successful we will be.

So we are committed to provide them the opportunity they need to stay current in an increasingly complex technology based environment.

And finally, we have embarked upon a significant restructuring of information technology management in governance that will strengthen, integrate and align our information technology management efforts across the Navy-Marine Corps team. A key element of that restructuring was the designation of Rear Admiral Tom Zelibar, the Chief Operations Director of Space, Information Warfare, Command and Control, and Brigadier General John Thomas, the Marine Corps Director and my colleague here today, to be dual hatted as Deputy CIOs for the Navy and the Marine Corps respectively, working with me. These designations will ensure that our information technology and command and control communications teams are truly aligned and providing the best value to the warfighter.

Again, thank you, sir, for your support of our information technology initiatives and our transformational agenda to achieve network-centric operations and knowledge superiority. I am happy to answer any questions that you have.

[The prepared statement of Mr. Wennergren can be found in the Appendix on page 503.]

Mr. SAXTON. Thank you, sir.

Mr. Gilligan.

**STATEMENT OF JOHN GILLIGAN, CHIEF INFORMATION  
OFFICER, DEPARTMENT OF THE AIR FORCE**

Mr. GILLIGAN. Thank you, distinguished members of the subcommittee. I appreciate the opportunity to address you today.

The Air Force is undergoing the most significant transformation in its relatively short history. This transformation is largely based on how we use information and information technology to increase our operational effectiveness. As an illustrative example, in Afghanistan information technology permitted us to combine precision guided munitions, rapid target identification to turn the Cold War era B-52 bomber into an effective platform for performing as close air support for small numbers of special forces on the ground.

Likewise information technology is permitting us to significantly shorten our air operations planning cycles and improve coordination of joint assets and forces in the current situation in Iraq.

Information technology is at the heart of every one of our warfighting systems. Within the Air Force we are now placing significant emphasis on improving the integration of our intelligence, command and control, and surveillance systems. Our goal is to leverage the power of modern information technology, including implementing what we call machine-to-machine communications to horizontally integrate information available in our joint and coalition air, space and ground assets. This permits us to shorten decision cycles and improve the quality of information available to commanders.

In support of this objective, we are investing in improved flexible communications links with our airborne platforms, enhancing our command and control systems to better leverage commercial standards and technologies, upgrading our base infrastructure to permit us to fully exploit DOD bandwidth expansion programs and improving the capabilities used to protect our networks and systems from cyber attacks.

The Air Force operates using the Air and Space Expeditionary Force, or AEF construct. We support overseas commitments by rotating AEF organization units from fixed bases usually on a 90-day cycle. In support of that we deploy forces and equipment worldwide, leaving many of the support functions at home. Moving information rather than people reduces airlift and logistics required as well as the cost of operations.

It also improves the decision-making by linking experts real time across geographic distances using our Department of Defense global networks. Our Air Force Global Combat Support System, or GCSS, program is central to our ability to link Air Force users worldwide. Using a standard Web browser based interface called the Air Force Portal and Web enabled applications, GCSS Air Force allows our airmen to access information and services worldwide on a 24-hour a day, 7 day a week basis. The online capabilities available through the Air Force Portal organize over 50 combat logistic services such as aircraft maintenance, status and spare parts ordering and tracking as well as over 100 self service capabilities for personnel pay, medical and other support functions.

By leveraging commercial Internet technologies and changing our operational paradigms, we are getting Air Force members out of the customer service lines and back on the flight line; in other



words, IT initiative consolidation of the management and operation of our many networks and servers. We have completed the consolidation of over 70 percent of our existing network and servers to date and we project we will be almost 90 percent complete by the end of this year.

By reducing our hardware inventory and standardizing system operations we have already been able to return to core mission functions, man-hours equivalent to over 1,000 man-years. We continue to work to enhance the tools, processes and personnel skills that we use to protect our systems and networks. We know that our adversaries are working hard to exploit vulnerabilities and destruct our military networks.

In 2002, we monitored 4.4 billion suspicious connections, a four-fold increase over 2001. Most suspicious activities were dealt with quickly by terminating the offending connections with no operational impact. However, we did have 93 events that resulted in some compromise of information or denial of service. This was approximately the same number as we had in 2001.

To continue our transformational efforts to support the expeditionary forces of the future I see a number of opportunities and challenges ahead. The ability to support information dominance through network-centric operation demands a highly skilled work force. Retaining our highly skilled work force in a competitive industrial market environment is a continuing challenge for us. We are using a variety of methods, including bonuses, to retain our experienced personnel.

In parallel, we are also looking to leverage industry capabilities to perform some information technology functions currently performed in-house. Our objective is to free up some of our military and civilian IT professionals to align them with higher priority missions. However, we are finding that the current legal and policy framework makes outsourcing enormously complex and that it takes far too long to accomplish, often 2 to 3 years.

Finally, by leveraging commercial capabilities and software products, we find that we also reap the consequences of the poor quality of current commercial software products that have numerous logic flaws that could permit compromise of our systems and interrupt our warfighting capabilities. We are now spending more money to patch flaws in these commercial software systems than we pay to purchase the system. I believe that poor software quality is a national crisis and deserves the attention of our government and corporate leadership. I personally talk with software vendors about this issue, but your support could assist us in this endeavor.

Although there are significant challenges that we are addressing, the Air Force is proud of the progress that we have made in leveraging information IT technology to increase our mission capabilities and improve cost effectiveness of our support activities.

This concludes my testimony. I would be happy to answer any questions that you may have. Thank you.

[The prepared statement of Mr. Gilligan can be found in the Appendix on page 484.]

Mr. SAXTON. Thank you, sir.

And General Thomas.



**STATEMENT OF BRIG. GEN. JOHN THOMAS, DIRECTOR FOR  
COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS  
(C4), CHIEF INFORMATION OFFICER FOR THE MARINE  
CORPS**

General THOMAS. Good afternoon, Mr. Chairman and members of the subcommittee.

Mr. SAXTON. We save the Marines for the last.

General THOMAS. I will try to keep it short then, sir.

The Marine Corps strategy is a very simple one, and we have heard a number of the issues that the Marine Corps is currently working with our sister services. The Department of Defense as well as Marine Corps strategy is built on three principles: Build the network, exploit the network and defend the network.

The network consists of people, Command and Control (C2) nodes, weapons systems and weapons platforms. Building a network involves having well-educated, well-trained, well-motivated people, and the Marine Corps is marching smartly to make that happen.

Another aspect of building the network is technology. The Marine Corps program currently has those programs in place and allows us to build that robust integrated seamless network that Mr. Stenbit talked about earlier. We talked about the joint tactical radio system, the communications program and the bandwidth expansion programs. All of these efforts are designed to allow to take us and push power to the foxhole. Building a network is about pushing power to the foxhole.

To exploit the network we need command and control tools that allow the operators, the commander out there to make decisions. Programs like the Global Command and Control System, the Global Combat Support System, the Unit Operations Center, the Deployable Joint Command and Control System, all these programs are being fielded with the intent of providing commonality and joint interoperability horizontally across the force.

To defend the network not only requires technology but it also requires training and education of our Marines. The Marine Corps has an initiative that we are proud to highlight. Our information assurance program where we are sending staff Non Commissioned Officers (NCOs) to the Air Force Institute of Technology to gain degrees in information assurance is just one example.

So exploiting the network and defending the network are key components as well. The Marine Corps has a program in place and we are happy to say that with your support we will continue to move forward and provide the support to the warfighters in the future.

Mr. Chairman and members of the committee, those conclude my remarks. I will be happy to answer any questions.

[The prepared statement of General Thomas can be found in the Appendix on page 519.]

Mr. SAXTON. We thank you very much for your comments. Could each of you share with us your service's IT investment strategy and how your goals match up with the process through which you procure technology that is needed? Why don't we start with Mr. Gilligan?

Mr. GILLIGAN. I would be happy to do that. Following on the distinction that Mr. Stenbit made, the distinction between our business and infrastructure and our warfighting within the Air Force, approximately half of our \$6 billion budget is strictly warfighting, approximately half is business and infrastructure, infrastructure which Mr. Stenbit put in his 70 percent figure. I distinguish them a little bit differently for a reason. As CIO I focus a lot of my attention on our common use infrastructure, which is our base capabilities, classified and unclassified, as well as our business systems. We spend a little bit less than \$3 billion in that area, and my objective in terms of the strategy is that becomes a relatively fixed investment for the future.

That has been the characteristic in the budget in the last couple of years. And my intent is that what we do is look for opportunities within that budget to reprioritize, to be able to modernize some of our business systems, to make additional investments in our infrastructure, to be able to basically reduce the cost of those capabilities, and thus far we have been able to do that.

On the other side, the warfighting side, we have actually seen some growth in those expenditures and capabilities, but that is to be expected. In fact, that is where we would like to continue to invest. It is that investment that is giving us increased capabilities in our warfighting area. For example, about half a billion dollars of increase in our budget was directly attributable to the Airborne Warning and Control System (AWACS), increased tempo of operations (OPTEMPO) of AWACS, data link enhancements, improved mission planning capabilities, et cetera. And each of those are looked at in terms of a cost-benefit analysis in terms what is the operational benefit. But in many cases we are getting significantly improved operational capability and in a few cases actually relieving, reducing the numbers of people required to perform those functions. So that is a top level strategy, sir.

General CUVIELLO. Mr. Chairman, the way we approach it is from an architectural standpoint. The architectural process has the first thing when you have a requirements generation by the users, whether the users are warfighters or business stewards, and that operational architecture is the first one. That is how I want to do my business, how I want to warfight, do personnel, logistics, et cetera. Then we talk walk down to the system as architecture, which is then how do the technologists apply technology to the solutions to those requirements that are based in an operational architecture. How we leverage that is that we are the proponents for the technical architecture, and that is all the standards and protocols, and this is called the joint technical architecture. So it is not service unique. It is from the joint perspective and from Office of the Secretary of Defense (OSD) and then try and apply across the board what is needed.

Now, the things that we control, we control the command and control systems, the warfighting aspects, because each one of the services are fairly different in the way they do their warfighting. The thing that is the real challenge is on the business side, because there is not much that we can do with our personnel and logistics and finance because it is all a defense activity. And that is what Mr. Stenbit was talking about, is that trying to get that operational

architecture of how I want to do finance business within the Department and logistics business, and then it works its way on down.

I know that what was being referred to in the General Accounting Office (GAO) report is that we each have lots of little systems out there in each of those areas. The reason why is because there is no operational architecture. People have gone to the systems architecture and said I need this function to happen right here, right now, on this post or in this function, and they come up with their little software program and then we have all kinds of black boxes that tie it together.

General CUVIELLO. So that is how we are managing from the standpoint of where do we want to put our resources. We want to put them in enterprise solutions to things on the business side of the house. And then on the warfighting, as I mentioned, we have—and that is what we call our objective force and our future combat system. And we are starting, as I mentioned in my comments, right from the ground as to how we want to warfight and then we come in and say, okay, here is what technology can do for you and then put the money to it.

Mr. SAXTON. Thank you. I am going to excuse myself for a few minutes to make a telephone call that I must make, but Mr. Wilson is going to take over for me.

Mr. WENNERGREN. We each have a similar situation in that our IT budget does include a large portion of money going toward direct warfighting systems. So our approach has been one of looking at end processes. On our warfighting side, we have our FORCENet construct, which is an enterprise architectural view and operational construct to look at mission capabilities from end to end, understand those processes and then make these smart investments that will get you the systems and capabilities to meet those processes.

Also recognizing the importance of our business systems, too, though, we have created a set of functional area managers that I mentioned in my opening remarks, and we have given these functional area managers the responsibility to look after that portfolio of applications, the entire logistics domain, the entire manpower domain, regardless of what organization originally generated a requirement for a manpower system. And by having that sort of portfolio management strategy in place they are able to make decisions that have allowed us to reduce the number of applications we have in each of our business areas.

Each of us of course as CIOs have the Clinger-Cohen Act responsibility to make sure the investments are happening correctly, and we are able to manage and monitor that process. But as part of our restructuring effort in the Navy and Marine Corps team, we have also added in this idea about an enterprise implementation plan, detailed guidance to our commands and system buyers of what is the right type of investments to make to match our IT strategy for the future so they can know their dollars are being spent in a way that will make sure that we have a joint solution that is knowledge centric, Web based in the future.

General THOMAS. Similarly the Marine Corps marches in step with the Department of Navy. Our requirements are clearly con-

cept based and capabilities based and we are constantly looking for the enterprise solution. The Marine Corps has taken the lead, as some of you may know, in having the first enterprise network capability in the Department of Defense. We also have published an IT capital planning and investment strategy which for the E business side of the house lays out the ground rules for how we should do business. As a CIO, I have also laid out an IT procurement strategy. OIT procurements come through the CIO of the Marine Corps. Similarly, we stood up an information technology steering group to take and help review all of our IT purchases, ensuring that we are getting the best bang for the buck. We also initiated activity based costing so we can associate a dollar value to the IT procurements that we are pursuing.

And as the Army has done, we have implemented an enterprise architecture effort where we are developing those operational system and technical architectures that allow us then to take and understand how these new capabilities will plug into the overall architecture.

Mr. WILSON [presiding]. Thank you very much, and at this time, I will recognize the Congressman from Minnesota, Mr. Kline.

Mr. KLINE. Thank you very much, gentlemen, for being here. Because of my background I guess I want to talk about the Marine Corps program for just a little bit. General, you are marching in step with the Department of Navy and I appreciate that very much and I am sure you are working together very closely. You did say, however, that you have put together an IT procurement strategy for the Marine Corps, I assume. And the dollars for that—those are green dollars that you get through Marine Corps programming?

General THOMAS. The—for the IT side of the house, that is correct, with a couple of exceptions. All of the crypto modernization is funded with blue dollars, or Navy dollars. The only other exception is that there is a small piece associated with the Navy-Marine Corps Internet that is funded with blue dollars, again, talking specifically about IT now.

Mr. KLINE. And I am a little bit interested in your IT steering group. Who is on that?

General THOMAS. We have representatives from the advocates throughout our departments. We have, you know, the ground combat element advocate, the command element advocate, the aviation combat element and the logistics command or logistics advocate. These are all three-star advocates. We also have representation from the operating forces that make up this information technology steering group as well as representation from the requirement side of the house.

Mr. KLINE. I like the coordinated approach there, but I am just interested because I recall so vividly now, it has been a long time ago, 15 years ago when the Marine Corps was trying to put together a strategy for modernizing—we just called it sort of computers, we needed computers back in those days. And the approach was so slow and so tedious and required winding through so many folks by the time we decided what we were going to do, everybody in the Marine Corps had gone through a couple of generations of buying computers just to get things done. Can you bring me into the modern world?



General THOMAS. We definitely changed a great deal since then. All Marine Corps computer procurements are funded centrally now. You are absolutely correct, sir, it used to be where the commanders out there would use their Operations and Maintenance (O&M) dollars to buy computers and what we were finding was that it eventually starts to cut into readiness. We moved into centralized procurement just as we moved to an enterprise network to ensure that those resources are not impacting readiness.

Mr. KLINE. I applaud that as long as it is fast and I assume that would apply to all the services that probably dealt with this at some way or another or some time or another where the centralized process was simply too slow. So I guess I am asking for assurances that while it is great to be centralized and have some commonality and not eat up O&M funds that could have been better used for training or other purposes, that you all feel like that it is responsive and fast enough and you don't have people sitting out there snapping their pencils and chafing at the bit saying we are 5 years behind date on our hardware or software.

General THOMAS. Absolutely, sir. And I can tell you that the current process that we have in place is very responsive. Of course, as you know, we will migrate or we have started to migrate to the Navy-Marine Corps Internet. And again that holds the opportunity to have an even greater refresh rate than what the Marine Corps was able to program for on its own using its enterprise approach. And of course the Navy-Marine Corps Internet is a Department of Navy-wide enterprise to take in and address those kinds of issues you were talking about.

Mr. KLINE. Thank you very much. I yield back.

Mr. WILSON. Thank you. And gentleman, I want to let you know that I have been a real beneficiary of the Web sites that you helped establish. And as a JAG officer, the JAG Web sites have been very helpful in being able to call up will forms, download them immediately, prepare wills particularly for persons being deployed recently. It has been very helpful and as you run into people between different States, it is particularly helpful, and also guidelines for rules of engagement, it just goes on and on how helpful what you are doing and how it makes all of us confident of the ability of our military.

But I do have concerns and may have been addressed really to the first panel more, but in terms of security. Again, I am concerned about that and what safeguards are made. And as a novice in all of this, it would seem like to me that clutter itself would add to the security. And if all of the military personnel have cell phones or hand-held computers, that it would be extremely technologically difficult to penetrate or understand. Could anybody comment on that?

General CUVIELLO. I guess I will start with like as an example our portals where people go in to do all the self-service applications to things like that. It is secured. It is triple secured, sort of like when you do your credit card for Amazon.com. Our e-mail now is all encrypted using public key encryption, using our common access card that all the Department of Defense is moving towards. And we are trying to from a—in the unclassified world use encryptions to



help us out. And of course on the secure side, everybody is on the secret side of the house.

When it comes to the wireless devices, as General Raduege mentioned, we are all also moving toward the encrypted ones, using the Cryptoberry not just the Blackberry, using the Sectera and other phones that are able to be secure. And it is a regular cell phone that you can talk secret on and all these are National Security Agency (NSA) approved. As we move more and more open to the Web base, our security from cyber warfare is at risk and there are a lot of issues, and I won't walk you through all those things that we are doing in the information assurance area.

Mr. WENNERGREN. Mr. Congressman, if I could add on to that a little bit, the power of these public infrastructure digital certificates is really central to our digital security efforts. I mentioned the common access card, the smartcard we are giving out. It has changed my experience both from a physical and cyber security aspect. When I walk in the building, I use this card not only to get myself in the building, but I go up to my office and use this to cryptographically log onto the network in a much more secure way than user IDs and passwords.

I then use the power of these digital certificates to be able to sign e-mails to prove that it really was David Wennergren that sent you the e-mail. I can use the digital certificates to encrypt information. I can use the digital certificates to launch myself to secure Web sites so I can have a secure transaction with a Web site to do a transaction that I don't want other people to get in the middle of. And when I came out to come to this hearing I pulled the card out of the machine. It locks up and nobody else can be me.

So as we continue to leverage the use of these certificates, we are working and talking with our industry partners to say things like, hey, you do wireless devices. If you had a smartcard reader on that device you could use the power of these certificates to add an additional level of encryption to the wireless signals.

Mr. GILLIGAN. If I could add an additional comment in endorsing the comments made by my colleagues but also adding another dimension, the specific question you focused on was the ability to in a very cluttered communications environment focus on perhaps intercepting a particular communication. And your premise is right to a degree; that is, it does get fairly complex if your objective is to try to intercept. And of course the cryptographic capabilities we are using mitigate largely against that. But one of our biggest threats now is not the intercept but is denial of service, and that is if an adversary can time the exploit of vulnerability or weakness to perhaps not compromise any information, but prevent us from using the systems that we are depending on, that can be in fact in many cases more damaging to operational effectiveness than the compromise of information. And so there are really several dimensions of cyber security that have to be addressed kind of in unison, and each of us have programs to try to deal with not just the protection of information from compromise, but protection of our systems and networks from denial of service or other attacks so that we can withstand those types of what is an increasingly frequent occurrence, as I mentioned in my testimony, where we are seeing these types of attacks.

Mr. WILSON. What I was envisioning is we are dealing with terrorists and they appear to be sort of low tech individuals as opposed to a superpower that could monitor everything is what I am hoping we can evolve. And really in line with what Congressman Kline had already indicated an interest in, and that is you work so closely with the private sector IT virtually seamlessly and the lag time—is there a lag time in working with the developments of technology, change in technology and is there anything we can do to help you overcome any red tape or hindrances to working with the private sector?

Mr. GILLIGAN. I would echo a comment that I made in my oral testimony. Today what I find in the Air Force and I am sure the other services see as well is the most frequent avenue for attack against our systems, that in most cases, as you point out, it is from a relatively unsophisticated group is exploiting publicized software vulnerabilities in our commercial products that we get from Microsoft, Cisco and Oracle. About one a day of these flaws are discovered. They are published. They are published on hacker sites along with the software that you can use to exploit the vulnerability, and it becomes a race situation for us to go and patch these systems. Now we are talking about software programs that have many millions of lines of codes. So it is impossible for us to go through them and find out where these logic flaws are. So it becomes a discovery process of finding and patching and fixing and trying to outwit, you know, the speed with which somebody can exploit.

I think the software industry is awakening to this as a problem, but it is something that really needs a lot more emphasis and we need to change the fundamental business paradigm that through the 1980's and early 1990's was speed to market and quality was second order of concern. Now we are reaping some of the benefits of that and we need now to change the dynamics and quality of the software. It is important for us to being able to protect our system.

Mr. WENNERGREN. Industry partnerships are tremendously important to us and when we are able to leverage best practices in industry that is when we get our best solutions. So the only thing I would ask is your continued support of the types of initiatives we are working, like the Navy-Marine Corps Internet, which really have leveraged best industry practices to help us keep that fresh technology in place.

Mr. WILSON. Thank you all again for your service.

Mr. SAXTON [presiding]. Mr. Wennergren, the Navy IT budget increased from 4.1 billion to 6.1 billion over a 2-year period. Given the NMCI contractor's experience of continually discovering more local systems, tell us what the Navy did to define functional requirements before you let this contract and where are you now on this.

Mr. WENNERGREN. Yes, sir, Mr. Chairman. It is at a very important point. As we rolled out this enterprise network it has done a tremendous thing for us. Besides just the value of the contract in terms of access and interoperability, it has served a wonderful forcing function. One of the forcing functions was actually finding all those applications. When you had hundreds of disparate networks that were local and not visible, it is very easy for commands to build applications and use them locally and, you know, through no

fault of their own good intentions, we would build the same applications over and over and over again. By moving to an enterprise network structure we are able to get that visibility, and it was that shock of how many applications really had developed over the course of the years that led us to this legacy applications rationalization process.

So it has done two great things for us over the last 6 months. It has allowed us to assign functional managers that say you have to look at those 3,000 applications within your domain and work that down to a reasonable number because I don't need multiple solutions that do time and attendance.

Mr. SAXTON. Just from a common sense point of view wouldn't it have been better if we identified these systems that we were going to integrate before we bought the system to integrate them?

Mr. WENNERGREN. That is the best approach and that is the approach that we really try for. And I think some of the things we are doing now with portfolio management and our FORCENet structure that we are actually looking at processes before we go buy new things. That is going to help us do a better job of that.

Mr. SAXTON. You have a complicated job. General, can we talk about future combat systems for a minute? Boeing was in the other day and they brought their charts with them, and when I look at that system or the proposal for such a system, I guess one way of saying it is it makes me nervous and the reason it makes me nervous is because we become so dependent on the technology, which is very useful but does that dependence on technology worry you at all?

General CUVIELLO. It worries me because there is a lot of unknowns out there because a lot of this technology is still sorting itself out. But if we don't move in this direction—I mean right now, today, over in Southwest Asia we are dependent on technology. Now it is current technology. There is some proof of principle and prototype technologies that we are using over there, but situational awareness, blue force tracking, being able to know where piece parts are as compared to 12 years ago, I mean the difference between 12 years ago and now is it is like a miracle. What we are trying to do is take those lessons learned and in the future be able to lighten up, lessen the footprint, and some would say trading iron for digits. Now I also have a lot of the iron guys that say, you know, digits haven't killed too many people these days, but that is all about precision. You have to do things more in precision and no longer in mass, mass fires versus precision fires.

So I believe that the technology will get there, that we will be able to take this net-centric, knowledge-based construct and architecture and then apply different kinds of weaponry to it than we have today. It is stepping out of the box. I know that is what you are referring to. But I believe that the technologies are coming along and that we will be able to do it in the future.

Mr. SAXTON. Forgive me for oversimplifying these kinds of situations, but I have to look at them from my perspective and here is what makes me nervous. I have a sailboat and on my sailboat I have a Global Positioning System (GPS) and I have a radar and all of a sudden I found out I can feed input from the GPS and the radar into my laptop computer and buy a system, a software sys-



tem to put in the laptop computer that would integrate all three systems. And every once in a while the screen goes blank and so I found out to keep my compass in good shape and to keep my paper charts on board, and I sure wouldn't want to be out in the ocean on a trip and have a storm come along and have that system crash and not have my paper charts and compass. That may be a simple way of looking at this, but that is the first thing I thought when I saw those Boeing slides of this tremendously integrated system of systems, worries the life out of me and maybe I shouldn't be worried, maybe I am just old fashioned and don't understand how this technology goes together, but that worries me.

General CUVIELLO. It is a concern because we are not comfortable. It is all about change, change management. Sort of like when computers came in. We could not get rid of typewriters. I mean we couldn't. Well, now you try and find a typewriter, you can't find it. In our—as an example in our digitized division, the 4th Infantry Division, in the backroom they always kept the maps and the grease pencils besides these flat screen displays with all the great technology on it. I will tell you what, they are taking very few of the grease pencils and the maps with them because they are very comfortable with the kind of technology that they have and it is going to take time. And I think over time that you will become more comfortable with the situation, too. I agree, we have not stopped training map reading and compass use.

Mr. SAXTON. On the other hand, on the positive side at least from my point of view is I live next door to the AEGIS integration facility up in Morristown and we have developed a great deal of confidence in that system. So I guess it is kind of a different application of very similar technology.

General CUVIELLO. Absolutely.

Mr. SAXTON. Any more questions from anybody? Well, listen, thank you for being here.

Let me ask you one other question, and I don't know whether you have input on this or not. But General, on Future Combat System (FCS) again, somebody was here to testify the other day and they happened to mention that the family of vehicles would be vehicles that would average about 20 tons. Are you——

General CUVIELLO. Yes. That is within the framework.

Mr. SAXTON. This isn't exactly your area?

General CUVIELLO. Let me tell you, I sit in on enough meetings on this.

Mr. SAXTON. I say this whenever I get a chance to say it, because I want everyone to know that we are concerned about this weight problem, and there are a couple of things that ought to get back to the right people in the Pentagon. One is if it is going to be 20 tons, then we got to buy enough big airplanes to carry them because the C-130 doesn't do it. I have been with Air Mobility Command (AMC). I have asked them for examples. I have been on board a C-130, the Stryker, which weighs real close to 40,000 pounds. I have talked to the pilots of C-130's and I have been out to Scott via telephone and received information back on how far a C-130 will fly with 40,000 pounds on board and how much fuel you have to offload the wings so you can take off on various lengths of runways, and 40,000 pounds is too heavy for a C-130 to be a func-

tional, deployable situation. So if it is going to weigh 40,000 pounds we ought to buy enough C-17s to carry it.

The second issue is a more positive one, and that is that it appears that the Army has developed knowledge about processes to process titanium and in conjunction with titanium producers that could provide us with a huge advantage, and I guess that is probably not in your bailiwick either but whatever we can do to promote that notion would be good because it really is all part of the same system and obviously we want it to be as capable as possible.

General CUVIELLO. Absolutely.

Mr. SAXTON. Thank you all for being here. I appreciate it, and I know the other members of the committee appreciate it, too, and we look forward to working with you in the future as we move down the road and learn more all the time.

Thank you.

[Whereupon, at 5:30 p.m., the subcommittee was adjourned.]





---

---

# **A P P E N D I X**

APRIL 3, 2003

---

---



---

---

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

**APRIL 3, 2003**

---

---





**Statement of Chairman Jim Saxton  
Subcommittee on Terrorism, Unconventional Threats and  
Capabilities**

---

**Subcommittee Hearing on Department of Defense's  
Information Technology Program and Policies for Fiscal Year 2004**

---

**April 3, 2003**

**Chairman:** Gavel down. Brings meeting to order.

[Makes the following statement.]

Good afternoon ladies and gentlemen. The Subcommittee on Terrorism, Unconventional Threats and Capabilities meets this afternoon to consider the Defense of Defense's Information Technology Policies and Programs for the fiscal year 2004 budget request.

The Department of Defense annually invests billions of dollars in information technology (IT) to support its business operations, and plans to invest similar amounts in fiscal years 2003 and 2004. The Defense IT budget request for fiscal year 2004 is approximately \$28 billion. This

is a sizable amount of funding for IT programs, systems, and services that needs to be properly managed at both the Department and the service Chief Information Officer (CIO) levels.

Technology changes and evolves rapidly and its integration is equally complex, thereby raising concerns that if IT programs and investments are not wisely planned with sound best practices coupled with an investment strategy—they are doomed to fail with costs of billions of dollars. This is a critical issue for DOD because its past investments have met with only limited success. The subcommittee is concerned that one reason for this lack of success may be attributed to the fact that DOD does not have a corporate blueprint or enterprise architecture to guide and constrain its IT investments in a manner that promotes interoperability and minimizes duplication and overlap.

DOD is now developing a department wide enterprise architecture that encompasses seven functional areas: (1) accounting; (2) collection, accounts receivable, and cash management; (3) financial and management reporting; (4) human capital management; (5) logistics; (6) procurement, payables, acquisition, and disbursement; and (7) strategic planning and budgeting. The subcommittee is interested to learn from the witnesses what progress the Department and the individual services have made in regards to each of these functional areas.

Secretary of Defense Donald Rumsfeld has stated on multiple occasions that IT is the enabler behind the defense transformation. What is needed today is the ability to leverage the technology to ensure its operational capability in both a business and warfighting environment. While the subcommittee recognizes the critical efforts and difficulty of IT modernization, concerns have been raised that there is not sufficient oversight and administration at the Department nor at the service CIO levels to achieve the objectives contained in the Department's enterprise architecture.

The General Accounting Office (GAO) has recommended that the Department develop an enterprise architecture and the investment management controls for effectively implementing the architecture. GAO also recommends that DOD should limit its IT investments to: (1) deployment of systems that involve no additional development or acquisition cost, (2) stay-in-business maintenance needed to keep existing systems operational, (3) management controls needed to effectively invest in modernized systems, and (4) new systems or existing system changes that are congressionally directed or are relatively small, cost-effective, and low risk.

The subcommittee is interested to learn more about how DOD and the service CIOs are managing their IT plans, programs, and processes,

and if the enterprise architecture is broad enough to give the Department and service CIOs the authority to effectively oversee both DOD's Corporate Transformation and DOD's Force Transformation (Command and Control). This hearing will attempt to determine how successful are the Department and the services at modernizing its IT business systems, and how effective and efficiently is it delivering the necessary IT tools and systems to the warfighters.

FOR OFFICIAL USE ONLY  
UNTIL RELEASED BY THE  
HOUSE COMMITTEE  
ON ARMED SERVICES

**STATEMENT OF**  
**JOHN P. STENBIT**  
**DEPARTMENT OF DEFENSE**  
**CHIEF INFORMATION OFFICER**  
**BEFORE**  
**THE HOUSE ARMED SERVICES COMMITTEE**  
**TERRORISM, UNCONVENTIONAL THREATS AND**  
**CAPABILITIES SUBCOMMITTEE**  
**APRIL 3, 2003**

FOR OFFICIAL USE ONLY  
UNTIL RELEASED BY THE  
HOUSE COMMITTEE  
ON ARMED SERVICES



Mr. Chairman and Members of the Subcommittee:

I am pleased to appear before the subcommittee this afternoon to discuss the Department's vision and key transformation efforts relative to the Department's communications and information technology. In addition to articulating the vision and the basic principles underlying it, I will briefly describe some of our key initiatives aimed at making the vision a reality.

As the Department of Defense (DoD) Chief Information Officer it is my job to provide leadership and overall direction to create a secure, assured enterprise infrastructure needed to enable network centric operations in warfighting as well as business functions. The vision, one that is shared by my DoD colleagues here today, is to create an environment where *"people throughout the trusted, dependable and ubiquitous network are empowered by their ability to access information and recognized for the inputs they provide."* In other words, we want to have an information environment where people fully utilize the network that they can trust in and depend upon; and their performance is not limited solely by the capabilities that are under direct command, but rather they benefit from the global reach of the network and all the other capabilities that are connected by the network. We are committed to doing what must be done to:

- Make information available on a network that people depend on and trust;

- Populate the network with new, dynamic sources of information to defeat the enemy; and
- Deny the enemy comparable advantages and exploit weaknesses.

In essence, we want to create an environment where the following five key architectural tenets prevail:

- "Only handle information once." Collecting information or entering data multiple times is costly and adversely affects efficiency in both combat and business operations. "Only handle information once" requires that processes be re-engineered, and that technology and processes are integrated to minimize time and effort dedicated to data collection and entry.
- "Post before processing" means that access to data for disparate needs is not delayed by unnecessary processing. Everyone is a provider and consumer of information. As a provider, they have the responsibility to post data before they use or manipulate it; as a consumer they will have the technical capability to securely access the data they are cleared to access when they want it and in the format they need.
- Users will "pull" data as needed instead of having massive amounts of information "pushed" to them regularly, regardless of whether it is needed.

- Collaboration technologies will be employed to assist users in making sense of the data that is pulled. For example, subject matter experts from diverse units or organizations are frequently called upon to come together to make sense out of special situations. The ability to pull expertise from within a unit, as well as from across the Department is a value-added feature of a net-centric environment.
- A reliable network is key. Diverse information pathways must be in place to ensure this reliability. Networks and systems must have security designed in and information assurance must be considered with interoperability as critical to ensure their 'net-readiness.'" Therefore, interoperability and information assurance must be the rule and not the exception.

The Department has undertaken a number of initiatives that will fundamentally change the way that we organize and fight in the Information Age and how we manage and assure our information resources that support the warfighters. These initiatives provide a solid foundation for DoD's net-centric transformation, and can be categorized into five key investment areas:

- Communications, or the Transformational Communications Architecture, consisting of the Global Information Grid Bandwidth Expansion, the Joint Tactical Radio System, and the Advanced Wideband System and Transformational Communication Satellite efforts.

- Enhanced computing capabilities organized into a Net-Centric Enterprise Service.
- Application and collaboration tools and techniques including Horizontal Fusion and distributed, global command and control systems.
- Data Management and Business Modernization efforts that enable data visibility and understandability through, for example, the use of metadata.
- Information protection and computer network defense techniques and technology engineered into and integrated with each of the above programs and initiatives to ensure Information Assurance.

**Transformational Communications Architecture:** The Transformational

Communications Architecture defines the transport element of the Global Information Grid (GIG) and will be composed of three fully integrated segments. The terrestrial segment will be based upon fiber optics and include the GIG Bandwidth Expansion. The wireless or radio segment will be based upon the software programmable Joint Tactical Radio System. The space-based segment will be composed of several systems with the Advanced Wideband System serving as a gap-filler while we pursue the objective Transformational Communications Satellite capability.

GIG Bandwidth Expansion (GIG BE): Current telecommunication lines are not robust enough to handle the volume of information needed to facilitate optimum, strategic decision-making. The GIG-BE is designed to be robust enough to address current bandwidth constraints. It will use advanced fiber optic backbone and

switching technology to upgrade telecommunications lines at DoD's critical installations, and provide networked services with unprecedented bandwidth to operating forces and operational support activities. The GIG- BE will provide approximately 100 times the current telecommunications capacity to critical Defense sites around the world. An increase in capacity of this magnitude will permit dual use of the bandwidth – with warfighting command, control, and intelligence functions as a primary mission. New security technologies are being developed to keep pace with expanding capacities and enhance performance.

Installation Bandwidth Modernization: Complementing implementation of GIG-BE will be Service-specific efforts to upgrade base or installation level communications capabilities to guarantee connectivity and ensure maximum benefits are obtained from the GIG-BE initiative. Accordingly, DoD Components are developing installation bandwidth expansion strategies that will provide a bridge from the installation or base level telecommunications infrastructure to the expanded GIG.

Joint Tactical Radio System (JTRS): The radio-based or wireless segment will migrate to the software radio-based JTRS technology. Software radios are essentially computers that can be programmed to imitate any other type of radio, thus, they can be readily configured to operate in different networks based on different standards. The JTRS radio will also be capable of acting as a gateway between users with different hardware radios – a capability that speeds the transition to universal interoperability.



Advanced Wideband System (AWS) / Transformational Communications

**Satellite (TSAT):** The space-based segment of the transformational communications architecture is critical because many users are deployed in areas where optical fiber is unavailable, and many of our information sources, particularly intelligence, surveillance and reconnaissance capabilities, are airborne – making them especially difficult to link into a wideband network. AWS will, in essence, extend the network's full capabilities to mobile and tactical users. TSAT will expand AWS capabilities and incorporate internet protocol and laser communications capabilities into the Department's satellite communications constellation.

**Net-Centric Enterprise Service (NCES):** The NCES provides a common set of information capabilities for the Global Information Grid to access, collect, process, store, disseminate and manage information on demand to warfighters, policy makers, and support personnel. These capabilities will enable decision cycles to be shortened by providing near real-time connectivity and computing power for warfighters and other users to get the right information, at the right time, in the right format to meet operational, tactical and mission support needs.

**Horizontal Fusion:** Networks are essential to a net-centric environment; but they have limited value without quality data that are reliable, accessible and usable in an integrated manner. The Horizontal Fusion Initiative will provide tools and means that integrate the smart "pull" of data with expert interpretations of the information. It is

aimed at providing the tools that allow users to identify what data is available, access it, smartly pull and fuse it, and make sense of the data gathered. These tools will require investing in data content and management, as well as the acquisition of commercial applications. Although the initial focus is on intelligence RDT&E, lessons-learned from the intelligence community will be exported to and employed by the DoD business communities such as finance, logistics, and personnel.

**Data/Information Management:** Computers and communications networks process, transport and deliver data. Horizontal fusion tools provide the means to search for, pull and fuse data from a myriad of sources, and allow users to make sense of data. Clearly, the crux of it all is "the data" – its visibility, accessibility, trustworthiness and understandability. Accordingly, the DoD Data Management Strategy has evolved with several features that we will promote and implement. For example, it emphasizes the use of catalogs, registries and other "search" services so that users can discover the existence of data with or without prior knowledge of its existence. It addresses means by which data is posted, tagged, advertised, retrieved and governed, as well as methods that facilitate trust in the data.

**Business Modernization:** I would be remiss if I did not address the business community because they are the people that support the warfighter; the net-centricity principles that we are applying to C4ISR, likewise, must be incorporated in business functions. The Under Secretary of Defense (Comptroller)/Chief Financial Officer is leading an effort to transform business processes. The CIO community's involvement

includes assessment of architecture products for compliance with the Global Information Grid architecture; promoting business process improvements and ensuring that net-centric architectural tenets are reflected in these improvements; system acquisition oversight; and providing for the IT infrastructure and ensuring that its capabilities are in sync with the business functions' requirements for these capabilities.

**Information Assurance:** The vision, *"people throughout the trusted, dependable and ubiquitous network are empowered by their ability to access information and recognized for the inputs they provide,"* holds profound implications for the Department's information assurance program. Because trust and confidence in our information is a primary concern when developing and deploying the information network and providing needed services, none of our critical systems, networks, platforms, and sensors should be deployed without the necessary security and interoperability capabilities to make them 'net-ready'. As such, our information assurance program has developed a strategy that supports this concept and has focused on providing the Department with robust protections, agile network defenses, integrated situational awareness, transformational assurance capabilities, and a professional, highly aware and trained workforce. Each of these elements works together to provide the necessary dynamic and agile information assurance capabilities for a network centric force. I view these capabilities as integral to our efforts to transform the communications capabilities of the Department and see information assurance as critical to successful business and war fighters operations.

Lastly, but no less important than other elements of my vision described above, people are the "edge" in "Power to the Edge." They are the "committed" providers and consumers of data, and the ones who must make sense of it; the program managers who must acquire IT within cost, schedule and performance goals; and partners, stakeholders and beneficiaries of what a net-centric environment offers. A thorough understanding is a prerequisite for commitment. We must promote and build this understanding. We must have a concerted, orchestrated, concentrated and sustained campaign of awareness to get people on board, educate and train them, and ensure that we all are working toward the net-centricity vision and goals from the highest levels on down.

I certainly welcome the support of this Subcommittee and look forward to a continuing dialogue regarding this critical area. Thank you.

For Official Use Only  
Until Release by the  
Committee on Armed Services  
United States House of Representatives



**STATEMENT FOR THE RECORD**

**BY**  
**REAR ADMIRAL NANCY BROWN, USN**  
**VICE-DIRECTOR FOR**  
**COMMAND, CONTROL, COMMUNICATIONS,**  
**AND COMPUTER SYSTEMS**  
**JOINT STAFF**

**BEFORE THE 108<sup>TH</sup> CONGRESS**  
**COMMITTEE ON ARMED SERVICES**  
**SUBCOMMITTEE TERRORISM, UNCONVENTIONAL THREATS,**  
**AND CAPABILITIES**  
**UNITED STATES HOUSE OF REPRESENTATIVES**  
**3 APRIL 2003**

For Official Use Only  
Until Release by the  
Committee on Armed Services  
United States House of Representatives



**Information Superiority, Information Assurance, and  
Information Technology in support of Joint Warfighting  
Requirements**

Mr. Chairman, Members of the Committee.

Thank you for the opportunity to provide testimony on the important topic of Information Superiority and its central role in supporting the Chairman of the Joint Chiefs of Staff, General Myers', top priorities of winning the Global War on Terrorism, enhancing Joint Warfighting capabilities, and Transformation. I am Rear Admiral Nancy Brown, the Joint Staff Vice-Director for Command, Control, Communications, and Computer Systems. My testimony will address Information Superiority, focusing on the delivery of assured, protected connectivity to increase combat power for today's warfighter as well as its vital role in the transformation of our Armed Forces. To demonstrate how Information Superiority supports the Chairman's priorities, I will discuss an overarching concept that guides all our Command, Control, Communications, and Computer (C4) investments commonly referred to as "net-centric operations," as well as its enabling infrastructure known as the Global Information Grid (GIG). Finally, I will share with you some of the important progress we have made over the previous year, and I will identify many challenges we face in achieving true Information Superiority.

Today is an unprecedented time in our nation's military history. Our entire Armed Forces are engaged, throughout the world, in battles every bit as demanding as any we have ever participated in. And while the War on Terrorism remains our primary focus, we are aggressively transforming our military capabilities to meet the challenges of the 21st Century. To guide the transformational efforts, the Chairman of the Joint Chiefs of Staff published his overarching vision, *Joint Vision 2020* (JV2020), which describes warfare in the information age. It articulates a vision for future warfare where Information Superiority is the *fundamental enabler* of the four pillar warfighting concepts: Precision Engagement, Dominant Maneuver, Focused Logistics, and Full-Dimensional Protection. In simple terms, Information Superiority means getting the right information to the right people, at the right time, in the right format, while denying an adversary the same capability. The investments we have made in Joint C4 capabilities, whether near-term efforts supporting the War on Terrorism or long-term transformational initiatives, are mutually supporting and all build towards enabling "net-centric operations." In short, our near term efforts are dramatically increasing the capabilities of our combatant commands today while establishing the foundation for true transformation and, in fact, moving some of the capabilities of the Global Information Grid to the left. Let me start my discussion by providing a basic overview of the Chairman's

priorities.

### **The Chairman of the Joint Chiefs of Staff's Priorities**

As a result of our nation's unprecedented strategic environment, the Chairman has established three priorities: To win the war on terrorism, to improve joint warfighting, and to transform our nation's military to face the dangers of the 21<sup>st</sup> Century. These priorities also reflect the priorities of the Secretary of Defense. Combined with the President's vision, the Department's leadership, the support of Congress, and the selfless service of our Nation's Soldiers, Sailors, Airmen, Marines, Coastguardsmen and Civilian workforce – our nation's Armed Forces continue to make progress in each of these areas.

**Global War on Terrorism:** The Chairman's priority to support and win the Global War on Terrorism needs little explanation. For the past 18 months, the U.S. Armed Forces, in concert with other federal agencies and our coalition partners, have conducted a determined campaign to defeat the most potent threat to our way of life – global terrorist organizations and the nations that harbor them. Clearly, the winning of this war is our most pressing priority.

**Enabling Joint Warfighting:** The U.S. Armed Forces' ability to conduct Joint Warfare is better today than anytime in our history; however, many challenges remain. Today, our Joint Team is founded on

the individual warfighting capabilities of the Services. To improve our Joint Warfighting capabilities, we must maximize the capabilities and effects of the separate units and weapons systems to accomplish the mission at hand – without regard to the color of the uniforms of those who employ them. This challenge demands that we integrate Service core competencies together in such a way that makes the whole greater than the sum of its parts. Our critical command and control information systems and networks must allow us to integrate our operations, and not simply deconflict them.

**Transformation:** As the U.S. military meets the challenges of the 21<sup>st</sup> Century, we must transform how we organize, support and fight as Joint Warfighters. Transforming the Joint Force requires embracing change: intellectual and cultural, as well as technological. We are in the process of revising our Joint Vision. This new vision will provide a broad description of what our Armed Forces can, and must become. In its broadest sense, this transformation transitions our Armed Forces to a capabilities-based force. Transformation is not a single thing nor simply new command and control or weapons systems. Rather, it is a holistic approach, requiring experimentation and assessment, which will result in changes to our doctrine, organization, training, materiel, leadership and education, personnel and facilities needed to create the future joint force.

**Realizing the Network - The Global Information Grid**

As the key enabler of Information Superiority, the Global Information Grid is the unifying program we are using to address each of the Chairman's priorities and, in turn, meet the operational requirements of our combatant commands. This 'building block' approach ensures that our combatant commanders have the tools that they need to effectively plan, coordinate and execute joint and multinational operations today, while also enabling tomorrow's transformation. We think of the Global Information Grid in the same way that most people think of the "Internet:" a single concept that describes something that is very complicated and constantly evolving. General Myers has stated that the GIG is a: *"Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information-on-demand to warfighters, policy makers, and support personnel."* It will enhance combat power through greatly increased battlespace awareness, improved ability to employ standoff weapons, employment of massed effects instead of massed forces, and reduced decision cycles.

The overarching rationale for the Global Information Grid is



supported by the ongoing shift to "net-centric operations" -- a true transformation in military affairs. In the military context, weapon systems are essential for mission success; however, a weapon system itself is not nearly as capable as a platform that is seamlessly linked to other platforms, all receiving the latest intelligence and command and control information.

For example, in previous 'platform-centric' operations, the links between sensors and shooters were tenuous at best and failed to meet the operational demands of our warfighters. In many cases, potential targets were 'missed' because the commander did not have the right information to make the right decision, at the right time. Nor did he have the ability to 'mass effects' because individual platforms rarely had the same view of the battlefield.

As we move towards "net-centric operations," the timely exchange of information will allow commanders in the field to leverage all available sensors and weapons systems in a synchronized fashion to dramatically increase combat power. The secure networking capabilities inherent in the Global Information Grid provide the fused, timely information essential for joint mission success. It enables commanders to create a dynamically integrated fighting force by linking sensors to shooters to generate massed effects. As you have seen on television lately, we have

made great strides towards achieving a net-centric force; however, doing business today is hard work! We must continue to work towards seamless interoperability that integrates the awesome capabilities of each Service into the joint team. I will address "net-centric operations" in additional detail when I discuss transformation.

As I discuss the role Information Superiority plays in achieving the Chairman's priorities, you will see that we are taking the first steps to realize the Global Information Grid today to support the Global War on Terrorism, while constantly keeping an eye on the big picture of transforming our forces. In short, the near term C4 investments we have made during the Global War on Terrorism have a two-fold effect: they satisfy critical near-term warfighter requirements while laying the foundation for the GIG.

### **Supporting the Global War on Terrorism**

The Department's top priority has been, and always will be, to defend Americans and U.S. interests. The events of September 11<sup>th</sup>, 2001, have demonstrated an increased and immediate need to improve our government's interagency information sharing capabilities. The rapid dissemination of information, through our country's vast technological superiority, will be the key to preventing, deterring and, in the worst

case, recovering from attacks on America.

Over the past few years, we have made tremendous investments to improve the command and control infrastructures required by our combatant commanders to fight and win this global war. In coordination with our Department leadership, we have undertaken the Global Information Grid Bandwidth Expansion initiative, which will provide a transport system that delivers high-speed internet protocol services to key operating locations worldwide, and will use leading edge technologies from commercial industry. This critical effort, which started this fiscal year (2003), is only a first-step towards realizing the GIG, but it also satisfies two critical warfighting requirements. First, it removes bandwidth as a constraint -- bottomline, it provides the combatant commander with the bandwidth and resources required to execute joint operations. Expanding bandwidth allows use of more robust information tools such as collaborative applications for command and control, and near real time video for Intelligence, Surveillance and Reconnaissance applications. Second, the GIG Bandwidth Expansion initiative provides a network 'redundancy' that ensures assured access to the network in the event of an attack or network failure.

To support the GIG Bandwidth Expansion initiative, we have also made significant strides to improve the Combatant Commanders' Theater

C4 infrastructures. This complementary effort allows our regional combatant commanders to modernize their respective C4 infrastructures to take advantage of the increased capacity provided by the GIG Bandwidth Expansion initiative or simply to replace outmoded or antiquated equipment.

Additionally, we have significantly improved the use of commercial satellite capabilities to provide the bandwidth required to operate in austere parts of the world. These efforts, based on the requirements of the individual commands, provide vital C4 improvements between the combatant commander and his subordinate commands and works towards extending the GIG to 'the last tactical mile.'

As we continue the Global War on Terrorism, a significant challenge we must address is the "stovepiping" of information within the numerous agencies throughout the Federal Government. The DoD is working collaboratively with Homeland Defense and other agencies throughout the government to ensure needed information is transferred across agencies in a seamless fashion.

The information mindset must change to embrace a "need to share" construct within our current "need to know" system. The DoD must engage with the Department of Homeland Security and the rest of the federal government to retain an information edge over an adversary

that chooses to remain in the shadows and attack our vulnerabilities.

We will still need to work hard at breaking down cultural and technological barriers between agencies to share command, control and intelligence data; it is critical that we are able to use the vast information resources throughout the federal government in a synchronized fashion.

Information sharing cannot be limited to federal and domestic agencies; we must also develop new ways and means to share information with our coalition partners and allies. As we continue to aggressively pursue terrorism across the globe, the ability to efficiently exchange information with our allies will allow us to decisively attack and destroy terrorist networks abroad.

Our increasing reliance on information resources and systems, combined with the growing number and sophistication of network attacks, underscores the importance of building a sound Information Assurance/Computer Network Defense posture throughout the entire federal government. In addition to developing safeguards against attacks, we must continue to develop the tools and techniques to rapidly detect intrusion, determine the source, and respond appropriately. The DoD clearly sees information sharing as a powerful enabler in the continuing Global War on Terrorism.



**Enabling Joint Warfighting**

We have made important strides towards solving the interoperability challenges of our legacy command and control, communications and computer systems while ensuring our future systems are 'born' joint. While we have achieved great progress in the development of truly 'joint' programs, the actual deployment of most of these systems takes time. To enable joint warfighting in the near and mid-term, we must continue to aggressively identify and resolve the 'seams and gaps' that exist in our current critical command and control systems.

The Joint Staff, in coordination with United States Joint Forces Command (USJFCOM), is working aggressively towards the Department's goal of seamless Command and Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) interoperability by fiscal year 2008. To achieve that goal, USJFCOM, working closely with the combatant commands, developed a prioritized list of critical command and control systems that have interoperability shortfalls to resolve. This prioritized list, endorsed by the Joint Requirements Oversight Council (JROC), allows the Department to concentrate its efforts on addressing the interoperability shortfalls most important to the combatant commands. Critical efforts such as the Family of Integrated

Operating Pictures (FIOP), the Single Integrated Air Picture (SIAP), Deployable Joint Command and Control (DJC2), and U.S. Joint Forces Command's Joint Interoperability and Integration (JI&I) will provide the Combatant Commander with a common operational picture of the battlefield. This picture, with a view of both friendly and enemy force locations, will enable seamless joint fires operational planning, coordination, and execution. As these efforts progress, USJFCOM will continue to set the operational requirements and prioritize the integrated architectures that will set the stage for future battle management command and control systems.

Recent events clearly highlight the need for systems that can support rapidly formed and deployed joint and coalition forces with "plug and play" ease and that are also fully scalable to respond to changing circumstances. The Deployable Joint Command and Control (DJC2) program will be such a system. This highly mobile command post configuration will support implementation of the Standing Joint Force Headquarters (SJFHQ) at each regional combatant command by 2005. In short, DJC2 is the material solution, providing both the command post infrastructure and command and control information systems, for the SJFHQ. Once fielded, DJC2 will be every bit as flexible and scalable as the forces over which a headquarters will exercise command functions such as processing intelligence, mission planning, and controlling

combat operations. U.S. Central Command (CENTCOM) is already employing a variation of the DJC2 concept to support operations in the Persian Gulf and the first DJC2 suite is scheduled for delivery in fiscal year 2005. We will use lessons learned from CENTCOM, as well as input from the other combatant commands, to facilitate the development, procurement, and deployment of this critical initiative.

As our experience in Afghanistan illustrates, our sea, land, air and space forces will be called upon to operate in areas with either primitive, or nonexistent communications infrastructures. In these conditions, the only viable communication path is via satellite. Military Satellite Communications (MILSATCOM) programs, coupled with commercial satellite capabilities, provide this vital support to our combatant commands. Over the past few years, we have made tremendous investments to expand the capabilities of our command and control infrastructure, including significant expenditures on leasing commercial satellite capacity. However, commercial assets cannot replace the secure, ready, and available access that military satellite communications can offer.

A graphic example of the increasing demand for bandwidth is clearly provided by reviewing the change over the past 12 years. Although the numbers of deployed forces in OPERATION IRAQI FREEDOM (OIF) are only half that of OPERATION DESERT STORM, our

bandwidth usage in OIF is more than 30 times as great. Use of vastly improved Intelligence, Surveillance and Reconnaissance (ISR) assets – such as Unmanned Air Vehicles (UAV's) like Predator – increase bandwidth requirements, but allow dramatically shortened decision cycle time in the targeting problem. Increased bandwidth also enables remote collaborative planning and information “pull,” which in turn allows synchronicity of effort, massed effects, and reduced personnel requirements in forward operating areas. “Net-centric operations,” as described here, require continued investments in military satellite programs to ensure future operations are not threatened.

### **Transformation**

Contemporary warfare presents us with security threats that are far more diverse, rapidly evolving and potentially more lethal than ever before. To develop the necessary flexibility and agility to respond to this broader spectrum of conflict, the Department must transform its forces and ways of fighting. The continued development and implementation of an operational Standing Joint Force Headquarters (SJFHQ) in regional combatant command theaters represents a critical initiative for joint force transformation. The area offering the greatest promise for true transformation in the near term is information sharing and the power of the collaborative environment.

The concept of "net-centric operations" will capitalize upon America's leadership in information technologies to blend current stovepiped systems and create information networks. These networks, all seamlessly connected with the Global Information Grid, will enable a coordinated exchange of information among the various levels of command at unprecedented rates. Transformation efforts are underway in the development of GIG enterprise services. These enterprise services, supporting the entire DoD and Intelligence Community, will provide a common set of interoperable information capabilities to securely access, collect, process, store, disseminate, and manage information-on-demand for Joint Warfighters, policy makers, and support organizations. These exchanges will give our warfighters the ability to mass firepower in time and space with a speed and accuracy that will overwhelm our adversaries' ability to respond. This fundamentally new way of employing joint forces can achieve such concentrations using smaller, leaner forces located in disparate parts of the globe, but able to collaborate in real time to coordinate devastating attacks.

Net-centric operation is not an exotic concept requiring decades of research and development. We can reasonably achieve a limited capability through the use of existing and emerging commercial off-the-shelf and military technology based on common open standards. Achieving this netted force and realizing its potential will require the



continued wise investment of resources.

The first steps on the road to a net-centric capability must be to make our legacy systems seamlessly interoperable, while ensuring that all future programs are "born" joint. Programs such as the Joint Tactical Radio System (JTRS) and the Mobile User Objective System (MUOS) represent true transformation and will provide the foundation for future joint and multinational operations. The development and maturation of joint programs has been, and must continue to be our focus in terms of supporting transformation efforts. For the first time, the Department will employ a single family of tactical radios, completely interoperable, to provide voice and data communications across all the Services -- truly a monumental effort. Additionally, we are aggressively pursuing the development and deployment of the Joint Command and Control (JC2) capability. This effort will provide a follow-on capability to the Global Command and Control System (GCCS) and will support command and control at the strategic and operational levels.

As I stated earlier, transformation is more than systems -- it is really a change in the way we think and act. In order to take advantage of the rapid technological advances that are taking place today, we must change our requirements and acquisition processes. Today, the Department is dramatically changing the way we do business. We have developed new processes and methods of determining weapon and

information technology systems requirements based on the capabilities and effects we want to achieve, rather than our current process which focuses only on the threats that we want to counter. This new process requires technical profiles for each newly designed system be created on-line, where we can test them for interoperability with other systems in this virtual environment before the system is even built. Two completely revised Chairman of the Joint Chiefs Instructions, CJCSI 3170.01C and 6212.01C, will be the vehicles we use to implement these changes to system development and interoperability.

The Department's significant investments in joint C4 capabilities reflect the importance of interoperable C4 systems in enabling the joint force. By employing this building block approach, we are able to address critical combatant command C4 requirements today and in the mid-term, each building upon the other towards a transformed, highly lethal and mobile force.

### **The Challenges Ahead**

There is no shortage of challenges and opportunities in the Information Superiority arena. I have discussed some of the challenges such as interagency information sharing and C4 interoperability that we face. Let me outline a few of the other notable challenges we face, with a special emphasis on Information Assurance.

The military and commercial sectors must co-exist. A strong economy and a strong military are both increasingly dependent on networks. In some cases, our information rides through the same pipes. In other cases, we are in 'competition' for resources that cannot be shared, such as frequency spectrum. Our weapons, systems, and operations are information intensive, and operational success requires military access to large bands of radio operating frequencies. The highly mobile, widely dispersed forces of the future will require even more spectrum in order to operate effectively and efficiently.

While we recognize the growing private demand for spectrum, we will pursue more efficient technologies, and continue to work with government agencies and private industry to develop mutually acceptable spectrum management solutions. We need to hold the line on the transfer of military spectrum to the commercial sector.

As discussed earlier, we must continue to balance investments in our satellite communications capacity as we move forward deploying the GIG. We have entered an era of great potential technological improvements, such as the Transformational Communications initiative in the satellite communications arena, that provide unparalleled promise for increased capability for the warfighter. We must aggressively pursue these new technologies, as well as

identifying, developing, and then sustaining the proper mix of military and commercial satellite capabilities, to ensure we meet the operational requirements of our tactical and strategic users.

As with interagency information sharing, we must also continue to improve our ability to interface and operate with our coalition partners. The challenge is obvious: when working with coalition partners, we must routinely strive to integrate multi-national technologies, most of which are developed outside of the U.S. It is imperative that we work with our coalition partners to develop the technological standards required to ensure the interoperability that the Combatant Commander needs for an integrated coalition command and control capability.

Information Assurance (IA) studies conducted over the past few years have provided ample guidance in determining the technology required for our defense-in-depth strategy. The challenge before us is to apply precious resources to field capabilities. We can't afford to allow the "best" to get in the way of the "good enough." The difficult part is determining the "good enough."

Joint directed exercises and training are critical evolutions in institutionalizing joint doctrine plus training/techniques and procedures associated with operating and securing our critical networks, and maintaining our Global Information Grid. Future exercises will focus on

specific cyber threats and risk mitigation techniques as well as dynamic allocation of network resources. We must expand these activities into the coalition-training environment.

Another area needing continued emphasis is our network “red teaming”—that is, our technical experts who attempt attacks and exploitations of our own networks. These teams are the method by which DoD assesses its network vulnerabilities, and our investments in this area are paying dividends. We know that no network is perfectly secure, and it is vital that DoD is adequately resourced to continue this process, and provide solutions to identified vulnerabilities.

Although DoD networks were not affected by the rash of recent attacks against commercial web sites such as E-Bay and CNN, DoD continues to see an ever-growing number of attacks against our information systems. It is time to reevaluate the penalties associated with deliberate hacking. The recent case law developed from malicious incidents such as the “Melissa” virus attacks, and numerous, highly publicized hacking events, provides enough evidence for the legal community to review current laws to determine if they are sufficient to deter future attacks against our systems.

It is important that we do not forget that people operate all of these systems. We cannot operate the Global Information Grid without highly



skilled people. We are using "special skill" rewards to attract, train, and retain our best Soldiers, Sailors, Airmen, and Marines. However, our Total Force Information Technology Warriors are faced with choosing between their military professions and opportunities in the commercial sector that provide pay compensation at a much higher level. We must continue to assess our retention programs, proficiency pay, and operational tempo, which affect this highly trained and experienced work force. They are truly our nation's most precious resource.

Finally, we cannot view the command, control, communications and computers (C4) systems and the intelligence, surveillance and reconnaissance (ISR) budgets as bill-payers for traditional weapon systems. C4ISR systems should be treated as the entry fee for transformation. And investing in these systems must be paid for up front.

### **Conclusion**

Ten to twenty years from now, I believe that people will look back on this period at the beginning of the 21<sup>st</sup> century and say one of two things. They will either say "There was a tremendous opportunity for

transformation – but it was squandered, because the true value of networking and connecting things in ways that allow them to function totally different than they had previously, was not appreciated.”; or...“It was realized that the single most transforming thing in our force was not a weapon system, but a set of interconnections that substantially enhanced capabilities, and by capitalizing on that awareness DoD and Congress, working together, made a difference.” It is my hope and belief that we will proceed down the latter path.

In conclusion, I believe we are making solid progress toward implementing a Joint Strategy for Information Superiority that supports our Warfighters. Mr. Chairman and Members of the Committee, I look forward to helping make the Information Superiority strategies that I have shared with you this afternoon a reality, and to addressing you in the future regarding our successes and the way ahead. On behalf of the Chairman of the Joint Chiefs of Staff, I appreciate the opportunity to present the Joint Staff's insights on how to advance this issue of growing national importance – Information Superiority.

NOT FOR PUBLICATION UNTIL RELEASED BY THE  
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE  
U.S. HOUSE OF REPRESENTATIVES

WRITTEN STATEMENT OF

LIEUTENANT GENERAL HARRY D. RADUEGE, JR. U.S. AIR FORCE  
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

BEFORE THE  
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES  
HOUSE ARMED SERVICES COMMITTEE

THURSDAY  
3 APRIL 2003

CLEARED  
FOR OPEN PUBLICATION

MAR 27 2003 7

DIRECTORATE FOR FREEDOM OF INFORMATION  
AND SECURITY REVIEW  
DEPARTMENT OF DEFENSE

NOT FOR PUBLICATION UNTIL RELEASED BY THE  
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND  
CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE  
U.S. HOUSE OF REPRESENTATIVES

03-C-0507

DRAFT

4/2/03 7:23 AM

**STATEMENT FOR THE RECORD  
LIEUTENANT GENERAL HARRY D. RADUEGE, JR.  
DEFENSE INFORMATION SYSTEMS AGENCY  
BEFORE  
THE HOUSE ARMED SERVICES COMMITTEE  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES  
SUBCOMMITTEE**

**INTRODUCTION**

Good afternoon Mr. Chairman, it is a pleasure to appear before the subcommittee today to discuss command, control, communications, computers (C4) and related issues. The Defense Information Systems Agency (DISA) is a combat support agency. As a combat support agency, our job is to support our Nation's Warfighters. Our core mission areas are global communications, joint command and control, joint interoperability, defensive information operations, and combat support computing. DISA has other responsibilities that include supporting the White House, facilitating the exchange of technical information within the Department and among our research and industrial partners, operating key eBusiness capabilities used across the Department, and providing enterprise acquisition services, but our Nation's armed forces remain our top priority.

To fulfill these responsibilities, we plan, develop, field, operate, and support command, control, communications, and information systems that serve the varied needs of the President, Vice President, White House Senior Staff, the Secretary of Defense, the Joint Chiefs of Staff, the Combatant Commanders and Joint Task Forces, deployed forces below the Joint Task Force (JTF) level, military departments, and other Department of Defense components. We provide this support under all conditions of peace and war.

DRAFT

Over time, the Secretary of Defense has chosen to provide these capabilities by means of a defense agency which can provide a single solution for DoD. These inherently joint and enterprise-wide systems and infrastructure enhance DoD interoperability, increase security, and obtain economies of scale. Moreover, by presenting a single DoD interface with our Nation's coalition partners and other federal, state, and local agencies, we help simplify the complex interoperability issues associated with coalition warfare and homeland security.

### **GLOBAL COMMUNICATIONS**

A trusted, reliable, and ubiquitous communications infrastructure is the foundation of information superiority and the essential prerequisite for network centric operations. DISA provides DoD's global classified and unclassified voice, data, video, and transmission services through a combination of terrestrial and satellite assets that are predominately commercial, though supplemented with military value-added features. Military value-added features include global reach and tactical extension, a defensive information operations capability, robust encryption, personnel and physical security, diversity for routing and media, precedence, interoperability, and visibility into the status of the network components in order to maintain reliability. These features are critical to ensure U.S. Forces are not denied access to information, geography, or space.

DISA manages the Defense Information Systems Network (DISN) -- DoD's consolidated, worldwide, enterprise-level telecommunications infrastructure. The vast majority of DoD's command and control traffic, voice conferencing, intelligence dissemination, and combat support



traffic travel over the joint networks provided by the DISN. It provides dynamic routing of voice, text, imagery, video, and bandwidth services. DISN services connect deployed forces to their home bases, combatant commanders, the military Services, and agencies. These long-haul services are the key to interoperability above the tactical level. Specific subsystems include the Defense Red Switch Network (DRSN) for classified voice conferencing, the Secret Internet Protocol Router Network (SIPRNet), the Non-Secure Internet Protocol Router Network (NIPRNet), the Defense Switched Network (DSN) for voice traffic, the DISN Video Secure Global (DVSG) service, Enhanced Mobile Satellite Services (EMSS), and network operations over the Defense Satellite Communications System (DSCS) and commercial satellite systems.

In support of the global war on terrorism, usage of these warfighting systems has increased dramatically since September 11<sup>th</sup>, 2001:

DRSN infrastructure has increased 400%

SIPRNET capacity has increased 292%

NIPRNET capacity has increased 509%

DSN infrastructure has increased 138%

DVSG (Secure) usage has increased 1150%

EMSS users have increased 300% and usage has increased 3300%

Satellite Bandwidth has increased 800%

Network-centric warfare demands that traditional communication seams between echelons, functions, and organizations be eliminated or minimized. A textbook example of this capability is DoD's EMSS program, which provides assured, global, secure voice, and unclassified data

DRAFT

4/2/03 7:23 AM

access to the DISN, Federal Government IT Networks, US-based Commercial Telephone Networks, as well as direct connectivity to other EMSS users. EMSS provides communications through the IRIDIUM commercial satellite constellation via a DoD owned and operated ground station, and is completely independent of local terrestrial telecommunications infrastructures. EMSS has experienced exponential growth in usage during the Global War on Terrorism. After September 2001, the number of users has increased 300 percent, with system usage increasing over 3300 percent. New usage records are set every month. For instance, March 2003 usage is expected to exceed 3 million minutes. Used for everything from humanitarian relief missions to military operations in Afghanistan and combat in Southwest Asia, EMSS provides effective, assured communications in support of current operations and is one of our most successful programs supporting warfighters today. The capabilities represented by EMSS are integral to the gains in precision, speed, flexibility, and tactical surprise essential for success in the global war on terrorism.

Although EMSS is a DoD-operated system, other federal government agencies have taken advantage of the unique architecture and assured connectivity provided by this system. Today EMSS serves as an emergency means of communication for National-level commanders and civilian leadership – providing the ability to communicate anywhere, at any time, through an assured network. Operationally, EMSS has been an unequivocal success – evolving into a critical communications infrastructure supporting U.S. Government operations throughout the world.

DRAFT

DRAFT

4/2/03 7:23 AM

To be effective, the DISN must assure connectivity with deployed forces in the tactical environment. A major initiative to improve access to DISN from deployed forces is the DoD Teleport program, which serves as the junction between space and terrestrial assets at six locations around the globe, giving deployed forces greatly expanded connectivity through the terrestrial DISN fiber optic infrastructure to information sources and support functions. When fully deployed, it will also cross-band among military and commercial SATCOM frequencies (L, EHF, Ka, UHF, Ku, C, and X) to enhance communications interoperability and provide greater flexibility and surge capacity. DISA is the program manager for Teleport, providing the design, integration engineering, and acquisition, with the military Services operating and maintaining the resultant product. Teleport implementation is defined in generations. Generation One is fielding Ku, C and X-band capabilities today. Generation One will be operational in 2003, with Generation Two and Three capabilities originally scheduled for completion in 2005 and 2010, respectively. However, the Combatant Commanders' requirement for these capabilities is so critical that the fielding of parts of Generation One was accelerated in support of operations in the United States Central Command (USCENTCOM) area of responsibility, and the OSD has recently approved accelerated fielding of key portions of Generation Two – the EHF terminals.

An improved joint enterprise network is a prerequisite to creating new synergies; taking advantage of all available information; and bringing available assets to bear in a rapid, precise, and flexible manner. Network improvements can reduce operational latency, surprise the enemy, and enable innovation while still supporting bedrock military functions. Mr. Stenbit has addressed the Global Information Grid Bandwidth Expansion initiative in his testimony.

DRAFT

## JOINT COMMAND AND CONTROL

DISA is a key DoD integrator for joint, coalition, and combined command and control (C2) and combat support capabilities. The integration of military Service and agency-developed data sources and decision support tools is essential to the combatant commanders' ability to "fight jointly." These products must support both fixed-base and deployed decision-makers on diverse platforms, and under communications conditions ranging from robust to austere. DISA's own joint C2 capabilities are focused on enabling the readiness, planning, mobilization support, deployment, execution, and sustainment of deployed forces. In addition, we provide the infrastructure that integrates military Service and agency products such as common distributed track object services, applications management, data access and translation, and collaboration services. We have three programs that provide joint C2, warfighter visibility into support functions, and organizational messaging services.

Through the Global Command and Control System-Joint (GCCS-J), we enable joint operations planning and execution (JOPES), global access to readiness data, situational awareness via a common operational picture, and collaboration and decision support capabilities for combatant commanders as well as many joint force commanders. GCCS-J components form the critical C2 backbone of joint operations and are deployed in more than 635 locations worldwide, supporting more than 10,000 joint and coalition workstations. Lighter, configurable deployments of GCCS-J – such as the Bosnia Operational Picture – support selected joint task forces and coalition operations. In support of Operation Enduring Freedom, we dramatically improved situational awareness, rapid application of combined force elements, and integration of intelligence in

planning and decision-making. Specifically, we accelerated the fielding of real-time Unmanned Aerial Vehicle video overlays, multi-source air pictures, intelligence and imagery data source integration, and unit track alerts to all levels in USCENTCOM, including Marine Corps units in the field, aboard aircraft carriers for strike planning, and at USCENTCOM headquarters for target planning and execution.

In addition to the accurate picture of the battlefield provided by GCCS, combatant commanders require accurate information on the status of combat support (CS) functions such as transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medical, and military personnel readiness in order to support operational objectives. Our Global Combat Support System (GCSS) provides this accurate picture. GCSS provides end-to-end information interoperability across and between CS functions. It supports the combatant command and JTF levels by supplying comprehensive CS information from reliable data sources. This access provides the warfighter with a single, end-to-end capability to manage and monitor units, personnel, and equipment through all stages of operations including monitoring, planning and execution, mobilization, deployment, employment, sustainment, redeployment, and force regeneration activities. By providing access to high-level integrated information and decision support tools, GCSS enhances the ability of combatant commands and JTF commanders to make timely, informed decisions. GCSS is integrated with GCCS to provide an enhanced picture of the battlefield along with decision support tools that enable military commanders to make timely, informed decisions. GCSS is here today. It is currently operational in seven combatant commands [USCENTCOM, USEUCOM, USJFCOM, USNORTHCOM, USPACOM, USSOCOM, and USSOUTHCOM], in Korea, and in the Pentagon's National Military Command



Center. In support of Operation Enduring Freedom, we rapidly developed and fielded enhanced GCSS capabilities to meet critical operational requirements from USEUCOM, USCENTCOM, and USSOUTHCOM. The result: GCSS reduced the time required to provide critical strategic airlift movement information from hours to minutes. Additionally, GCSS successfully supported USJFCOM's Millennium Challenge exercise, a large-scale joint field experiment that supports their strategic concept for future warfare -- rapid decisive operations.

The third C2 capability we provide is organizational messaging. Organizational messaging on a global scale requires a high degree of security for our troops and must ensure that the information they receive is accurate, reliable, and confidential. The Defense Message System (DMS) is a managed data messaging system comprised of message handling and transfer, directory, systems management, and security components. These components, particularly the messaging components, are derived from commercial products which have been enhanced to meet DoD messaging requirements including timely assured message delivery, message integrity and authentication, security, and positive identification of recipients. DMS is operational at 270 military installations worldwide.

## **JOINT INTEROPERABILITY**

Interoperability is the core of jointness. The most reliable strategy for achieving interoperability is the use of a common infrastructure and common infrastructure services wherever possible. Interoperability support for enterprise systems includes operating standards, developmental and operational testing, spectrum deconfliction and supportability, and optimization activities such as modeling and simulation. Weapon systems, sensors, and tactical assets are often highly

specialized with C4 capabilities embedded. Interoperability of these assets is a prerequisite for the gains in precision and timely integrated operational capability required. Enterprise C4 systems must also achieve this same degree of interoperability.

In close partnership with the combatant commanders, military Services, and other agencies, DISA provides several key capabilities focused to achieve platform, sensor, and unit interoperability among U.S. and coalition forces. These key capabilities and enablers ensure interoperability and security are built-in and maintained throughout the system life cycle and include: developing and maintaining warfighter interoperability standards; system information exchange and interoperability requirements assessments; interoperability testing and certification; on-site support for exercises and contingencies; and spectrum management and deconfliction.

We provide direct interoperability support to warfighters during contingencies and exercises by stationing interoperability liaisons on-site at key combatant commanders' and allied headquarters. We also provide 24x7, 365 days a year "Hotline" support and deploy "fly-away" response teams. For example, during Operation Enduring Freedom, 49 formal interoperability issues were resolved.

DISA is DoD's system certifier for C4I interoperability. We operate the Joint Interoperability and Test Command to accomplish this mission in close partnership with the military Services. In the last four years, 117 critical interoperability problems with significant operational impact were identified during this testing and certification. Testing and certifying that DoD information

DRAFT

4/2/03 7:23 AM

technology and national security systems meet their joint, validated interoperability requirements reduces risk to the warfighter. Through developmental testing, we encourage developers to build interoperability into their systems. Through exercise support, we facilitate maintaining interoperability throughout a system's life cycle.

As the DoD executive agent for information standards, DISA leads DoD's information technology and data standards activities for the Office of the Secretary of Defense, combatant commanders, military Services, agencies, and the international defense community. In many areas, DoD effectively meets its IT requirements through implementing commercial standards. However, tactical interoperability in critical combat missions can only be achieved through adopting and implementing a minimum set of technical, procedural, and operational standards on specific platforms that are explicitly military in nature. For example, Tactical Digital Information Links (TADIL), military symbology, and U.S. Message Text Formatting (USMTF) are military standards, and, as such, are absolute essentials for interoperability. The existence of a well-defined process and support structure for these standards was key to resolving a number of TADIL and USMTF interoperability issues during Operation Enduring Freedom. DISA serves DoD as a center of excellence for resolving interoperability concerns in a wide range of programs. We are deeply involved with two joint test and evaluation programs (JT&E) -- the Joint Shipboard Helicopter Integration Process (JSHIP) JT&E, which tests and evaluates joint service shipboard and helicopter interoperability, and the Joint GPS Combat Effectiveness JT&E, which tests and evaluates combat effectiveness of GPS in adverse jamming and interference environments.

DRAFT

DRAFT

4/2/03 7:23 AM

At the very core of combat effectiveness is the ability to communicate effectively. The essential element in any mobile communications grid or systems network is access to radio frequency spectrum. This vital and finite resource has seen its market value increase dramatically as technological advances lead to intense competition for its allocation and use in both the public and private sector. DISA supports the Secretary of Defense in identifying future spectrum requirements and developing policy recommendations to ensure DoD has access to the radio frequency spectrum necessary to execute the National Military Strategy.

Nearly every commercial and military piece of equipment deployed by the armed forces uses frequency spectrum or is affected by electromagnetic radiation. We help ensure that DoD systems function as planned, without suffering or causing degradation in the electromagnetic battlespace. A failure in this area can result in restricted operational employment, diminished mission effectiveness, or even the death of friendly forces. DISA's Joint Spectrum Center (JSC) works with the military Services and agencies to identify and ameliorate the risks related to adverse electromagnetic environmental effects.

## **DEFENSIVE INFORMATION OPERATIONS**

The DISA information assurance (IA) program is broadly focused on attack detection, designing proactive information protection, and information assurance. We secure DoD enterprise information systems and provide support to combatant commanders and deployed forces in securing their respective systems. We also provide capstone IA capabilities for the entire department such as the DoD Computer Emergency Response Team (DoD CERT); DoD-wide anti-virus licensing; DoD Public Key Infrastructure (PKI); and network accreditation and

DRAFT

certification processes, policies, and implementation. We have a core responsibility as the C3 Critical Infrastructure Protection (CIP) defense sector lead component.

Cyber attacks happen with great speed and stealth. Nonetheless, critical warfighting information processes must continue to function effectively while under cyber attack. The DISA information assurance strategy is based on the idea that defenses must stop most cyber attacks. These protection mechanisms include physical, electronic, and procedural components. To remain effective over time, the defenses must be kept current in the face of rapid evolutions of technology, attack strategies, and organizational change; this takes a significant technical and operational effort. However, defenses are never foolproof. Should an adversary breach these protections, DoD must have the capability to detect, contain, and respond to the attack. This entails high levels of situational awareness, significant analytical capabilities to characterize the nature and extent of an attack, formulation and coordination of effective courses of action, and the ability to rapidly execute approved courses of action across a global infrastructure. The tools and procedures required to accomplish both protection and reaction to attack in a highly technical, complex, joint, multi-organizational environment are correspondingly sophisticated. Our program recognizes the distributed nature of information system designs and is instituting the DoD IA services infrastructure needed to continue to interoperate and fight jointly while taking advantage of modern web-centric and network-centric technologies. Our efforts in this area include hardening joint enterprise capabilities through perimeter defenses, critical infrastructure protection, and security for specific high-value joint systems including the DISN, GCCS, DMS, and Combat Support Computing. Other efforts include:

DRAFT

- Providing IA services for the DoD Computer Emergency Response Team (DoD CERT), the Global Network Operations and Security Center (GNOSC), and USSTRATCOM's Joint Task Force for Computer Network Operations (JTF-CNO).
- Deploying, operating, and monitoring defenses and a sensor grid at key enterprise locations and gateways between DoD and others.
- Developing, deploying, and operating tools to coordinate attack analysis and response across various DoD operational entities.
- Providing direct assistance to combatant commanders for information assurance to include technical protection, assistance visits, and operational support.
- Developing and implementing a DoD-wide vulnerability management program to include vulnerability alerting, remediation procedures, a Defense Information Technology Security Certification and Accreditation Process (DITSCAP), and secure configuration standards.
- Developing, deploying, and operating the single DoD cyber identity credential infrastructure, the DoD Public Key Infrastructure, and a secure global directory service.
- Developing and deploying tools and security designs to enable coalition operations.
- And, providing site licenses for key joint information assurance tools and DoD-wide product licenses for anti-virus software.

The DISA GNOSC performs essential network management on a 24x7, 365 days a year basis across the DoD to ensure sustained and responsive integrated network operations. The GNOSC is the single network operations center in DoD with a composite view of unclassified and



classified global, voice, data, and video communications used for command and control. Its primary mission is to direct, manage, control, monitor, protect, and report on essential elements and applications of the GIG to ensure its availability. The GNOSC is manned by highly motivated, extremely competent communications professionals including both military and civilian personnel. The warfighter perspective is priority one to this mix of military and civilian personnel as they synchronize priorities across the GIG. In the event of a national emergency, crisis, or significant IA event, the GNOSC, in coordination with the National Communications System, DoD CERT, telecommunications industry, Internet providers, commercial CERTS, and the JTF-CNO directs actions across the GIG to either mitigate the event or respond to the crisis to protect DoD command and control communications.

The DoD CERT is charged with the global analysis of real or potential network security breaches threatening the GIG. Firmly postured with global visibility of DoD's 21 connections to the commercial Internet, the DoD CERT provides defense against cyber attacks targeting military networks. The DoD CERT identifies significant threats to the GIG and develops, disseminates, and implements timely countermeasures to these threats. In addition, the team assesses the incidents reported by combatant commanders, military Services, agencies, and regions individually and cumulatively for their impact on the warfighter's ability to carry out current and future missions.

The GNOSC and DoD CERT provide primary support to the JTF-CNO, which is the DoD's leading organization for computer network defense and attack operations. As the operational component for USSTRATCOM for Computer Network Operations, JTF-CNO has very

successfully defended DoD networks and operations, and prevented DoD operations from being affected by computer intruders, viruses, and worms. The GNOSC, DoD CERT, and JTF-CNO are collocated at DISA headquarters to provide the necessary synergy among the directing, analysis, and responding components of network defense. During the 2002 calendar year, GNOSC, DOD CERT, and JTF-CNO detected, analyzed, and responded to more than 46,000 events on DoD's unclassified networks. For example, on the evening of 24 January 2003, the GNOSC, DoD CERT, and JTF-CNO took action to issue port blocks at all NIPRNet gateways within 2 hours of the first reports of the Microsoft SQL (Structured Query Language) "Slammer" worm. The port blocks effectively prevented any further compromises of vulnerable DoD systems from the Internet. They also deployed signatures on intrusion detection devices to alert network security monitors across the globe of any Slammer related activity. The port blocks, in conjunction with the Information Assurance Vulnerability Bulletin released in September 2002, significantly reduced the number of reported infections within DoD. In fact, there were only 264 confirmed infections throughout DoD's 14,774 SQL servers compared to an estimated 75,000 infections on the Internet.

## **COMBAT SUPPORT COMPUTING**

DISA provides mainframe and server computer operations, production support, technical services, and end user assistance for command and control, combat support, and eBusiness functions across DoD. Combat support computing supports more than 700,000 users, operates more than 1,200 applications using more than 55 mainframes and 1,350 servers, 24 hours a day, 7 days a week, 365 days a year and supports both unclassified and classified computing environments. Our five Defense Enterprise Computing Centers (DECC) and their detachments,

rely on highly skilled and experienced teams of government and contractor personnel to operate hardware and software encompassing a broad spectrum of computing, storage, and communications technologies. DISA has "smartsourced" these activities, contracting out specific functions where appropriate.

DISA has demonstrated an auditable record of major end strength and cost reductions in the mainframe operating environment. Over the past 11 years, the number of processing sites has decreased by 97%, end strength has decreased by 90%, billing rates have decreased by 80% and operating costs have decreased by 70%, all in spite of a 60+% increase in mainframe workload. The latest customer survey shows that customer satisfaction ranks significantly higher than the average score for commercial service providers.

Our facilities have been designed and managed to provide a secure, available, protected, disciplined, and interoperable environment for both classified and unclassified processing under military control. As an integral component of the GIG, we provide global reachback, end-to-end control, defensive information operations, and operational sensitivity. Combat computing services also hosts GCSS databases, which provide commanders with web-based access to information on transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medical, and military personnel readiness. This avoids the need to air lift and support a considerable IT infrastructure in the area of operations.

DISA provides computer processing for the entire gamut of combat support functions to include transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medical, and

military personnel readiness. Some of the more important requirements supported by the thousands of applications being hosted in DISA facilities include:

- Providing command and control of warfighting forces
- Ensuring weapon systems availability through management and control of maintenance and supply
- Managing and facilitating mobility of the warfighter through management and maintenance of the airlifter and tanker fleets
- Providing warfighter sustainment through resupply and reorder
- Providing the warfighter with information on the location; movement; status; and identity of units, personnel, equipment, and supplies
- Managing the medical environment and patient care
- Supporting DoD business and eBusiness processes

These applications are developed by the military Services' and agencies' central design activities. Despite the lack of common development standards and the often disparate, stovepiped nature of these predominantly legacy applications, DISA provides common computing platforms, networks, and enterprise systems management tools that serve to standardize the underlying infrastructure and integrate the combat support business processes it supports. Using the global reachback provided by DISN, a deployed joint task force can "plug into" this common computing infrastructure to get full, interoperable support. Through GCCS, GCSS, and a common communications and computing infrastructure, DISA provides the joint warfighter with a single, end-to-end capability to manage and monitor units, personnel, and

equipment from mobilization through deployment, employment, sustainment, redeployment, regeneration, and demobilization.

Our computing facilities were designed to be highly available data processing centers. They are secure, capable facilities with dual, high capacity DISN connectivity, and organic defense-in-depth, resulting in a more secure and robust computing infrastructure upon which to build. They feature automated systems management to control computing resources and gain economies of scale. Additionally, we have aggressively pursued an assured computing philosophy designed to ensure information and mission critical applications are continuously available for customers.

#### **OTHER MISSIONS**

The White House Communications Agency (WHCA) provides normal and emergency information services, including non-secure and secure voice, video, and record communications; automated data processing support; and other services. WHCA serves the President, Vice President, White House senior staff, National Security Council, U.S. Secret Service, and others as directed by the White House Military Office.

The Defense Technical Information Center (DTIC) is the central clearing house for exchanging scientific and technical information between government and industry. DTIC acquires, stores, retrieves, and disseminates scientific and technical information to support DoD research, development, engineering, and studies programs. DTIC's users search databases containing technical reports, research summaries of work in progress, independent research and development summaries, defense technology transfer agreements, descriptive summaries, and

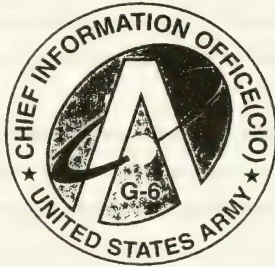
special collections. DTIC also hosts more than 100 web sites sponsored by the Offices of the Secretary of Defense, the military Services, and defense agencies.

Our Enterprise Acquisition Services establish and administer a family of contracts with commercial telecommunications companies worldwide to provide voice, data, video, and transmission services. These contracts include provisions that go beyond commercial equivalents in order to meet military requirements for priority service, surge capability, and encryption. Services procured on these contracts represent about \$100 million per month in usage fees. In addition, DISA offers a complement of information technology product and service contract vehicles to support end-to-end information requirements. From enhanced mobile satellite handsets, and satellite air time, to quick and affordable information technology solutions, we have contract vehicles available to support every telecommunications need, whether the support is to USNORTHCOM for domestic defense or to USCENTCOM for the War on Terrorism. These services are offered to both DoD and non-DoD Customers.

## **SUMMARY**

DISA exists to provide the C4 capabilities our Nation's warfighters and defense professionals require to execute any type of operation, from full-scale conflict such as Operation Iraqi Freedom to small scale contingencies such as operations in East Timor. We are committed to providing ubiquitous, robust, secure, joint, and interoperable C4 capabilities that are essential to our national security.





**STATEMENT BY**

**LTG PETER M. CUVIELLO  
CHIEF INFORMATION OFFICER/G-6  
UNITED STATES ARMY**

**BEFORE THE**

**SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL  
THREATS AND CAPABILITIES  
COMMITTEE ON ARMED SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES  
FIRST SESSION, 108TH CONGRESS**

**ON THE DEPARTMENT OF DEFENSE FISCAL YEAR  
INFORMATION TECHNOLOGY POLICY AND PROGRAMS**

**APRIL 3, 2003**

**NOT FOR PUBLICATION UNTIL RELEASED BY  
THE COMMITTEE ON ARMED SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES**

**STATEMENT BY  
LTG PETER M. CUVIELLO**

**ON THE DEPARTMENT OF DEFENSE FISCAL YEAR  
INFORMATION TECHNOLOGY POLICY AND PROGRAMS**

**Introduction**

Mr. Chairman and members of the subcommittee, thank you for the opportunity to provide testimony describing the Army's plan for transforming information technology in support of the overall Army and Department of Defense transformation efforts. All aspects of the Army transformation to a lighter, faster, more deployable and capable force hinge on the ability to move information, be it voice, data, video or imagery, from the lowest levels to the highest, seamlessly and in real time.

**Direction**

Congressional intent for the Army to transform Army information technology, management, and operations is clear. The 107<sup>th</sup> Congress Report 107-732 stated: "The committee believes that the overall interests of the Department of Defense and the Intelligence community would be best served by quickly moving to a network-centric environment." The report noted that significant benefits would accrue from this to include more effective use of data, more efficient and effective use of platforms and the ability to better use and protect resources.

The Army has completely embraced the network-centric concept and is making significant progress transforming our systems, platforms and processes to achieve network-centricity, interoperable in the Joint, Interagency, and Multinational environment. We are doing this today as exemplified in Southwest Asia and in our day-to-day operations.

In addition, the Army is also working to comply with all aspects of the Clinger-Cohen Act. Today, the Army Chief Information Officer (CIO)/G-6 sets the strategic direction and objectives for Army Command, Control, Computers, and Communications (C4) as well as provides supervision over all Army C4 and information technology functions. While we have made progress in transforming cold war command and control architectures, much remains to be done, and your help will be needed to allow us to continue the transformation effort.

## **Strategy**

Our Army Knowledge Management Strategy is five fold:

- 1) Leverage all information technology capabilities of the Department of Defense and The Army at the enterprise-level to reduce the total cost of ownership.
- 2) Integrate best business practices to promote Army transformation to a network-centric, knowledge-based force.

- 3) Manage the information technology infrastructure as an Army enterprise.
- 4) Implement a web-based enterprise knowledge portal to provide universal, secure access for the entire Army.
- 5) Harness the human capital of our Army IT workforce through effective recruitment, training, and retention of our soldiers and civilians.

**Leverage all information technology capabilities of the Department of Defense and The Army at the enterprise-level to reduce the total cost of ownership.**

The Army fully supports the collaborative effort to leverage defense-wide capabilities to improve operational efficiency while decreasing total ownership cost. We are developing and working with sister services on advanced communications systems that are critical enablers for the overall Department of Defense and Army Transformation efforts. These systems will provide the backbone for Objective Force information dissemination, for Joint netted Command, Control, Communications, and Computers (C4), as well as Intelligence, Surveillance, and Reconnaissance (ISR), and for scalable knowledge capabilities that are smaller, self-sustaining, modular, agile, and that meet bandwidth and services requirements from legacy to the Objective Force. These tactical systems are required to support secure, simultaneous real-time voice, data, imagery, and video at all levels while on the move, and include:

- **Joint Tactical Radio System: Interim/Objective Force Software Defined Radio**, multi-waveform, multi-mode tactical radio system to transmit voice, data, imagery, and video information.
- **Warfighter Information Network – Tactical: Objective Force** reliable, mobile high bandwidth wireless network to transmit voice, data, imagery and video information between the Future Combat System, Stryker Brigade Combat Teams, Army Legacy forces, Joint, Interagency, and Multi-national forces.
- **Future Combat System: Objective Force System-of-System** supporting embedded C4 and ISR capabilities.
- **Global Combat Support System – Army: A standard, web-based user application** providing worldwide access to support Combat Service Support users, such as logistics, personnel, and medical.

These systems are being developed to automatically establish ubiquitous networks with multi-level security, managed and defended as part of the overall enterprise, with knowledge-based processes to empower Army and Joint, Interagency, and Multi-national users. Objective Force C4 and ISR leverage reach-back and direct downlink capabilities for intelligence, force planning, administration, technical engineering, information operations, and logistic support.

## **Integrate Best Business Practices to promote Army Transformation to a Net-centric, Knowledge-Based Force**

The primary reason to share knowledge across the Army is to improve decision-making by getting better and faster information to the decision maker. In knowledge-based organizations, all processes, tools, and technologies are focused on exploiting the enterprise's knowledge assets to achieve mission critical objectives. Domination of situational understanding is essential to the operations of the Army's Objective Force. Commanders and their staffs must be able to "...collaborate with subject matter experts: subordinate, adjacent and higher commanders and staffs in real time...." In order to achieve the seamless "factory to foxhole" continuum of operations necessary for decision dominance, Army processes and systems must be transformed to improve timeliness, accuracy, and relevance of information critical to decision-makers at the point of decision.

Changing from a stovepipe culture that compartmentalizes information to one that values knowledge sharing and collaboration across the enterprise involves process change in how we create and access knowledge. The Army will transform and integrate processes to allow the sharing of knowledge across the organization.

The Army is moving to a performance-based enterprise through business process redesign, resulting in the Army Knowledge Enterprise Architecture, C4/IT Investment Strategy, and the use of Enterprise Resource Planning (ERP) and



similar systems. Business process redesign forces the Army to evaluate and improve both what we do and how we do it. With a focus on enterprise level service, this process led to the development of the Army Knowledge Enterprise Architecture (AKEA). Providing the blueprint for an integrated set of information systems (Systems Architecture), AKEA cuts across the functional “stovepipes” and Service boundaries and complies with mandated standards (Technical Architecture).

The C4/IT Investment Strategy is a systematic, integrated approach to resource management that identifies optimal combinations of investments to maximize value in a constrained resource environment. It considers economic value and Army leadership prioritization to generate best-value combinations of interrelated programs. This guarantees the best “bang-for-the-buck” at the enterprise level. Additionally, to more quickly and economically achieve an effective enterprise, the Army regularly considers the use of Enterprise Resource Planning (ERP) systems. These systems are commercial, off-the-shelf applications with pre-designed interoperability that can either be used as-is or modified to meet the needs of the Army. The greatest challenge in the employment of ERP systems is ensuring they meet the critical security needs of the Army Knowledge Enterprise Architecture.

**Manage the information technology infrastructure as an Army Enterprise.**

A successful enterprise is dependent on the infrastructure to support it. The Army's goal is to ensure no leader at any level is hampered within the decision making process by the lack of bandwidth. To ensure Army leaders can take advantage of the Department of Defense Global Information Grid—Bandwidth Expansion (GIG-BE) project, the Army must upgrade its supporting infrastructure. This ongoing effort, the Installation Information Infrastructure Modernization Program (I3MP), is an iterative process of infrastructure and connectivity improvement based on available resources applied against an enterprise level prioritization. While I3MP currently provides the "back-bone" (the information pipeline within the installation) upgrade, the Army is moving to achieve the efficiencies of also including the building-to-building upgrades in the same process, thus encompassing the entire enterprise as a whole.

Successful automation of the battlefield is dependent upon the ability to secure, distribute, and present information in a decentralized command and control environment. Networks and network-centric initiatives have no geographical boundaries, and warfighters worldwide, must rely on the physical architecture to consolidate, distribute, secure and manage this information. Commanders must trust the information made available, and that trust can only be afforded if proactive security measures and equipment is in place to protect it. We are acutely aware of our responsibilities to support Joint, Interagency, and Multi-national communities, and our commitment is one of unquestionable data integrity and information support. The Army is ensuring this capability through

the implementation of the Army Knowledge Enterprise Architecture (AKEA). The AKEA is the Army's portion of the Department of Defense Global Information Grid. The Army Knowledge Enterprise describes The Army's IT framework from the posts, camps, stations, National Guard armories, and Reserve Centers to the deployed combat forces.

As part of this Army Knowledge Management Strategy, we have established the Network Enterprise Technology Command (NETCOM) to act as the single Army network operator and defender. This command is the key operational element that will ensure the Army can provide full spectrum network operations across the broad range of command, control, and communications requirements facing the Army today. NETCOM will ensure the interoperability to meld separate Army components into a single, seamless network, centrally managed and protected, and capable of meeting requirements during battle or while managing crises in the homeland.

Pivotal to the protection of this network are the Army Network Operations and Security Center (ANOSC) and Computer Network Defense in the form of the Army Computer Emergency Response Team (ACERT). These two critical programs will provide continuous monitoring and cyber security capabilities, ensuring seamless and continuous coverage of the total Army network, from the foxhole anywhere in the world to the continental United States.

Additionally, security of access to the enterprise is improving, through the Department of Defense Common Access Card (CAC) program and the use of biometrics. The CAC will be the principal card used as physical identification, for physical access to DoD buildings, and as the DoD's primary platform for the public key infrastructure (PKI) authentication token. The CAC is to be issued and maintained using the Defense Enrollment Eligibility Report System and the Real-time Automated Personal Identification System (DEERS/RAPIDS) infrastructure, bringing increased efficiency, improved effectiveness, and operative information assurance. The CAC initiative is an initial step in making use of smart card technology across the functional areas of the Army and as part of the Army's larger efforts to incorporate electronic business throughout the service. Additionally, the Army is leading the way in the exploration and advanced use of biometrics (the use of unique physical characteristics for positive identification) as a means of secure access to the enterprise.

**Implement a web-based enterprise knowledge portal to provide universal, secure access for the entire Army.**

To allow this movement of information, the Army developed its principal gateway to information, Army Knowledge Online (AKO). AKO is a secure portal recognized as among the top ten in the country, through which more than one million subscribers pass to access increasingly vital information and on-line services. The Army Knowledge Online is our integrated enterprise portal for accessing information, conducting business, and managing operations. It provides worldwide accessible e-mail and data storage in the form of the Army

Knowledge Collaboration Center that allows our warfighters to share information, as well as limited access by family members. The principal challenge is the data processing site, which currently has no offsite, real-time backup and recovery capability. The Army Chief Technology Office is currently in the process of standing up a disaster recovery site that will provide a fully redundant fail-over function as well as an additional active processing capability.

### **Harness the Human Capital of our Army IT Workforce through effective Recruitment, Training, and Retention of our Soldiers and Civilians.**

The Army is improving not only the quality and protection of the structure of the network, but it also improving the quality and protection of its work force within the network. The Army is becoming more and more dependent upon information technology in both business and tactical applications, therefore the Army now provides critical training of information technology skills and IT security through the extremely efficient, web-based platform of E-Learning. Centrally managed, de-centrally executed, this "anywhere-anytime" approach provides unprecedented accessibility, increased productivity, and tremendous cost efficiency, moving training to the force, instead of moving the force to training.

### **Conclusion**

The future success of the Army depends upon its ability to transform, and we cannot afford to delay that transformation. The Army's C4 and information technology transformation provides the enabler for the Army at War and Army

Transformation. With the continued support of Congress, we will achieve our goal of a net-centric, knowledge-based Objective Force, and the Army will achieve its transformational goals, meeting Congressional guidance before the turn of the decade.



**Testimony of**

**John Gilligan**

**Chief Information Officer**

**United States Air Force**

**before the**

**HASC Subcommittee on Terrorism, Unconventional**

**Threats and Capabilities**

**3 Apr 03**

**NOT FOR PUBLICATION UNTIL RELEASED  
BY THE COMMITTEE ON ARMED SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES**

JOHN M. GILLIGAN



## BIOGRAPHY

UNITED STATES AIR FORCE

### JOHN M. GILLIGAN



John M. Gilligan, a member of the Senior Executive Service, is the Air Force Chief Information Officer, Washington, D.C. As the Air Force CIO, Mr. Gilligan is the principal adviser to the Air Force leadership on information management, business processes and information technology standards. He leads the Air Force in creating and enforcing IT standards, and promoting and shaping an effective strategic and operational IT planning process. He also leads the Air Force in acquiring IT systems. Mr. Gilligan works with Air Force management to ensure the conduct of IT processes is timely, cost-effective, follows all applicable statutes, regulations and policies, and provides the best available capability consistent with requirements and within available budget resources.

Prior to joining the staff of the secretary of the Air Force, Mr. Gilligan served as the CIO for the Department of Energy. In this position, he developed and directed the IT management strategies, policies and practices for the department. These responsibilities included year 2000 readiness; information protection; strategic planning; standards in computing, networking and security; establishment of system and information architectures; and

corporate information technology, capital planning and investment.

### EDUCATION:

- 1973 Bachelor's degree in mathematics, Duquesne University, Pittsburgh, Pa.
- 1976 Master of science degree in computer engineering, Case Western Reserve University, Cleveland, Ohio
- 1984 Master's degree in business administration, Virginia Polytechnic Institute and State University, Blacksburg

### CAREER CHRONOLOGY:

1. 1975 - 1977, systems analyst, System Development Corp., McLean, Va.
2. 1977 - 1978, technical staff member, Defense Communications Division, International Telephone and Telegraph, Nutley, N.J.
3. 1978 - 1981, branch manager for computer security projects, System Development Corp., McLean, Va.
4. 1981 - 1984, computer scientist, Worldwide Military Command and Control System, Information System Joint Program Office, McLean, Va.
5. 1984 - 1987, Deputy Director, Worldwide Information System Program Office, Hanscom Air Force

[http://www.af.mil/news/biographies/gilligan\\_jm.html](http://www.af.mil/news/biographies/gilligan_jm.html)

03/20/2003

JOHN M. GILLIGAN

Base, Mass.

6. 1987 - 1990, Director of Studies and Analysis, Air Force Communications Command, Scott Air Force Base, Ill.

7. 1990 - 1991, Director of Software Architecture and Policy for Command, Control, Communications and Computers, Deputy Chief of Staff for C4, Headquarters U.S. Air Force, Washington, D.C.

8. 1991 - 1992, Director of Resources, Deputy Chief of Staff for C4, Headquarters U.S. Air Force, Washington, D.C.

9. 1992 - 1998, Air Force Program Executive Officer for Battle Management, the Pentagon, Washington, D.C.

10. 1998 - 2000, Chief Information Officer, Department of Energy, Washington, D.C.

11. 2000 - 2001, Principal Deputy Assistant Secretary of the Air Force for Business and Information Management, and Deputy Chief Information Officer, Washington, D.C.

12. 2001 - present, Air Force Chief Information Officer, Washington, D.C.

#### **AWARDS AND HONORS:**

1991 Meritorious Civilian Service Medal

Senior Executive Service bonus awards

1995 and 2000 Presidential Meritorious Executive Rank Award

1998 Distinguished Civilian Service Medal, Joint Chiefs of Staff

1998 Presidential Distinguished Executive Rank Award

#### **PROFESSIONAL MEMBERSHIPS AND AFFILIATIONS:**

Institute of Electrical and Electronics Engineers

Armed Forces Communications and Electronics Association

(Current as of January 2002)



Mr. Chairman, distinguished members of the Subcommittee, I thank you for this opportunity to discuss the Air Force efforts and plans in the vitally important area of information technology and information assurance.

### **Overview**

The Air Force is currently undergoing one of the most significant transformations in its distinguished history. This transformation is leveraging the power of information technology to increase the effectiveness of our operational capabilities, in many cases permitting us to use our older weapons systems in ways that were never intended. For example, in Afghanistan information technology permitted us to combine precision guided munitions and rapid target identification to turn the cold war era B-52 Bomber into an effective platform for performing Close Air Support in our war on terrorism.

The experience gained by our senior leaders over the past decade in increasing availability of information to improve effectiveness of air and space operations, combined with the lessons derived from industry in leveraging information technology to improve effectiveness and efficiency of business functions, have accelerated the Air Force's efforts to embrace and exploit the power of information. Our strongest advocates of the need for improved information technology and associated advances in the management of information are our senior operational commanders who understand the operational importance of information and the potential of modern information technology.

Critical to the Air and Space Expeditionary Force (AEF) construct, our method of supporting overseas commitments by rotating operational forces from fixed bases, is the ability to rapidly deploy combat forces and equipment world wide, while leaving as many

support functions at home base. We link forward combat personnel to home bases through robust, global information systems, in effect permitting them to “telecommute” to the battle. Moving information rather than people reduces the airlift and logistics required as well as the cost of operations. It also improves decision-making timelines associated with expeditionary missions as we can very rapidly leverage our best experts in a cooperative manner.

In my testimony today, I will highlight how we are leveraging information technology to support Air Force, joint and coalition warfighters as well as to improve our combat and business support operations. I will also address our efforts to establish a true global network infrastructure that will support our warfighting and support functions.

### **Leveraging IT to Support the Warfighter**

As a part of our transformation, the Air Force is moving from a platform-based, static garrison force to a capability-based expeditionary air and space force. To guide our transformation and our investment decisions, we are specifying mission-oriented concepts of operations, or CONOPS, that define how we will conduct air and space operations with joint and coalition forces. A common characteristic across all these CONOPS is the need to provide the right information at the right time to enable commanders to make the right decisions. This permits us to achieve “information dominance,” that enables joint and coalition forces to prevail in any operational situation.

The significant challenge we face in achieving information dominance is the integration of manned, unmanned and space systems and the information they generate and process. The Air Force recently established a senior-level organization in the headquarters to focus Air Force efforts toward integration of these warfighting systems. This organization is the Deputy Chief of Staff for Warfighting Integration or Air Force “XI”. The Air Force XI

organization is focused on horizontally integrating our command, control, intelligence, surveillance, and reconnaissance capabilities that support air and space operations. As Air Force Chief Information Officer, I work closely with the Deputy Chief of Staff for Warfighting Integration to spearhead the integration and transformation to an information-driven, network-centric Air Force, while staying in harmony with the efforts of other services and federal agencies.

Achieving the goal of an integrated warfighting system by leveraging information requires that we enhance the exchange of information, moving from human-aided and driven information exchanges to true machine-to-machine communications. New technologies, evolving from the Internet such as so-called "middleware frameworks" and data exchange standards such as extensible markup language, or XML, permit us to design new systems rapidly. They also let us integrate information from legacy systems without major redesign. State of the art "data mining" technologies allow information to be automatically extracted and presented to decision makers rather than forcing operators to search manually for the information. In short, our objective is to permit our operators to practice the art of command by applying information technology to permit effective machine-to-machine interactions.

#### **Air Force FY 2004 Information Technology Budget**

The FY04 information technology budget reflects our priorities by focusing investments on critical systems essential to our expeditionary forces. The Air Force has requested \$6.5 Billion for Information Technology for Fiscal 2004. This is roughly 7% of the total AF Total Obligation Authority (TOA) of \$93.5B and an increase of \$.7B over the information technology budget approved for FY 2003. Approximately \$2.9B of the \$6.5B is for National Security Systems (warfighting) with the predominance of that funding budgeted for



Command and Control (C2) to include airborne platforms like the E-3 Airborne Warning and Control System (AWACS). Funding for information technology that support our business and combat support functions has been level or decreased from FY03 to FY04.

As a primary thrust of the Air Force's efforts to transform how we conduct military air and space operations, the Air Force is using electronically stored and transmitted information to shorten response times and deal with asymmetric threats. There are a number of budget increases that are focused on National Security Systems programs that support information dominance to include: the AF Mission Support System which supports detailed aircraft mission planning, Cheyenne Mountain/Tactical Warning and Assessment, Tactical Data Links, Global Broadcast Service, Joint Tactical Radio System for our Airborne systems, and command and control for our joint Combatant Commander. Information Assurance capabilities to protect our systems and networks is projected for increased spending including Joint Computer Network Defense resources for US Strategic Command and received additional resources for communications network infrastructure protection due to heightened threats.

Other budget increases reflect the fact that the Air Force recently became the Executive Agent for U.S. Northern Command, which resulted in funding additions for Command and Control and Information Assurance to support their homeland security mission. To ensure robust global communications for our forces, increases for our fixed and deployable infrastructure modernization are planned for FY04 through the Combat Information Transport System and the Theater Deployable Communications program. While there have been increases in our information technology budget, there are still areas where our investment and

modernization pace is slower than what our warfighters would like. These areas are highlighted in later comments.

#### **Supporting a Global Information Network**

Key to the Air Expeditionary Force concept is need for a reliable and robust network infrastructure that can connect our forces anywhere in the world, whether they are on land or in the air, and in the future even in space. We have traditionally looked at terrestrial communications, space-based communications, and airborne data links as three separate domains with different characteristics. We are now creating a single network that embraces all these media. Moreover, because the Air Force operates simultaneously from its stateside bases and forward locations in any operation, that network must be global in scope. To achieve decisive warfighting effects, the Air Force supports Department of Defense efforts to strengthen the Defense Information Systems Network by expanding use of fiber optics for terrestrial connectivity, as well as advanced satellite systems using radio, laser, and Internet protocol (IP) networking technologies. Our goal is to eliminate bandwidth as a constraint to the warfighter. The Air Force strongly supports the efforts of the Department of Defense efforts to implement the Transformational Communications Architecture and the Global Information Grid-Bandwidth Expansion (GIG-BE) initiative. These efforts, coupled with complimentary investments by the Air Force in our base infrastructure, will provide the information infrastructure for all military communications and enable what we call network-centric operations.

The Department of Defense Global Information Grid Bandwidth Expansion (GIG-BE) Program will provide a secure, robust, optical, Internet protocol-capable terrestrial network that dramatically increases world-wide connectivity to over 30 of our key Air Force bases, resulting in a hundred fold increase in capability. This increased bandwidth will enable

improved situational awareness by providing increased capacity for intelligence, surveillance and reconnaissance (ISR) information and allow better use of advanced capabilities for information fusion and collaborative planning. The expansion will also aid robustness by minimizing the risk of single points of failure and reduce the possibility of disruption to time critical functions.

The Air Force's complimentary component to the GIG Bandwidth Expansion program is the Air Force's Combat Information Transport System, or "CITS". The CITS program extends the GIG-Bandwidth Expansion into our bases. The focus of the CITS program is continued modernization of the information transport capability at the base and major command level, to include installing fiber in place of aging copper cabling, replacing older maintenance intensive equipment, replacing or upgrading existing voice switching systems, providing network control centers with the tools to manage and protect our information networks and systems, and providing information assurance tools. The CITS program will also be our vehicle to develop and increase our secure wireless capabilities for flightline and other areas best supported by wireless communications methods.

In addition, of the essential communication capabilities required to support future operations is more effective machine-to-machine communication, especially with our aircraft platforms. We are leveraging the flexibility inherent in current software programmable radio technology to maintain interoperability with legacy radios and are building a flexible networking capability that will transform the way we do business. To achieve this capability the Air Force has dramatically increased funding for the Joint Tactical Radio System in FY 04 and subsequent years.

The Air Force has also changed how we manage this global network. The global network requires an operational construct where commanders must be able to dynamically command, control, synchronize and integrate platforms, sensors and strikers on a secure global grid. The Air Force Chief of staff recently codified this concept as he directed establishment of the Air Force Net Operations Security Center, or "AFNOSC" to assume command over the operations of our global networks. The AFNOSC will have operational control over our base and command network control centers, as well as our cyber security capabilities within the Air Force Computer Emergency Response Capability. This organizational change ensures that the same command processes and disciplines that we use to manage our operational forces and weapon platforms will be applied to our critical networks and information systems.

#### **Air Force combat support activities**

The transformation goal applied to our combat support and business processes is to achieve significant improvements in operational effectiveness while reducing support costs. In this area, perhaps even more than in the operations domain, we are exploiting both the lessons and technology of commercial enterprises. A centerpiece for these efforts is our Global Combat Support System Air Force, or GCSS-AF, program. Through GCSS-AF, we are modernizing our combat support and business applications. This program is leveraging commercial web and Internet tools and technologies by providing a standard, web-based user interface for all Air Force users through the Air Force Portal. With the Air Force Portal, our airmen can now gain access to information and services worldwide, on a twenty-four hour a day, seven day a week basis. We are also exploiting commercial middleware framework technology to rapidly integrate our support and business systems and data.

Starting in 2002, Air Force members could access mission and self-service tools through the Air Force GCSS Portal right from their desktop or laptop computers worldwide. In addition, we have recently fielded a reduced sign-on feature within GCSS to eliminate the separate usernames and passwords that our airmen now have to remember for the variety of computer services.

Examples of mission tools supported in GCSS-AF include a virtual "work space" for each member; over 50 logistics services including aircraft maintenance status, fleet mission capable rates, supply management, spare parts tracking, transportation/vehicle management; and information regarding the planning and tracking for our Air Expeditionary Forces (AEF). This critical information available worldwide through our single portal interface links deployed forces with home bases: an all-essential element in the AEF concept.

In addition to the mission support capabilities just identified, the on-line capabilities available through the Air Force Portal organize over 100 self-service applications and tools with common look and feel. An example of a self-service tool that has provided improved quality of life for our airmen is the Defense-wide "myPay"--a system that allows the member to verify and track his/her own pay when at home or deployed. Another quality of life system available on the Portal is the "Virtual Military Personnel Flight"--a system that allows our people to readily obtain and update their military information, to review job announcements, obtain assistance on assignment changes including relocation, make medical appointments, and much more. With these self-service tools and others like them, we are getting Air Force members out of customer service lines and connecting them on-line where they can get things done faster and be even more productive in their Air Force jobs.

As we expand GCSS we are also integrating the many separate websites that exist across the Air Force, providing a common look and feel and simplifying web content management. We are also working to provide personalized workspaces that will recognize individual users and provide customized push/pull of job-relevant information utilizing triggers and alert notifications. We have plans in FY 04 to field a set of knowledge libraries to facilitate enterprise information sharing. Our ultimate goal for the Air Force Portal and GCSS is to provide our people with personalized, role-based access to information (on the network) that they can depend on and trust...to perform the tasks that our national defense demands of Air Force members whether at home or deployed.

#### **Server-Network Consolidation**

Our increasingly network-centric operation demands a robust, efficient, and common infrastructure that possesses the necessary performance and efficiency characteristics. Two years ago, the Air Force took an important step in achieving this capability by initiating a program to consolidate operations of our many separate networks and computer servers. Our initial focus was to centralize the operations of our on-base networks and computer servers. We have made tremendous progress. We are 70% complete today on the base network and server consolidation efforts and project we will be almost 90% complete by the end of this fiscal year. We have reduced the number of email servers by 78% (1,400 to 300). Similar efficiencies have been achieved in reducing web, file and print servers. In addition, we have achieved improvements in reliability and security because we can manage these network computers. Our support costs have significantly decreased especially with fielding of a standard desktop. We estimate that by reducing our hardware inventory and standardizing systems operations, we have already been able to return man-hours equivalent to 1,000 man-



years to core duty requirements. We further estimate an additional 1,000 equivalent staff will return to their core duties by the time we complete the consolidation efforts in FY 05, allowing us to leverage our human capital much more effectively.

Our consolidation efforts are also improving our ability to provide information protection for our networks and systems. As a part of consolidation, we are fielding state-of-the art network and systems management tools. These tools permit us to rigorously control configurations of our systems and to update our system configurations remotely. These capabilities are resulting in improved protection as well as reduced manpower requirements for software distribution, asset management as well as network and system troubleshooting. Our major command network operations centers can now rapidly push software patches to fix vulnerabilities or provide updates for anti-virus software. We can now have command-wide implementation of fixes in hours/day instead of the days/weeks it used to require. Our Air Education and Training Command alone is reporting savings of 450 hours per base per patch (approximately 20 patches per year.)

### **Information Assurance**

We continue to employ a multi-faceted approach to cyber-security based on a layered set of protection mechanisms as well as appropriate policies and guidelines. Our network-centric concept relies on the highest possible protection of our information and network systems used to store, process, and disseminate this information. At the same time, we know that our enemies are working to exploit vulnerabilities and disrupt our military networks. This threat continues to force us to rigorously track millions of suspicious network connection attempts every year. In 2002, of the 11 billion suspicious activities that the Air Force tracked, 93

required comprehensive investigation. Most suspicious activities were dealt with by quickly terminating the offending connection with no operational impact. However, we did have 29 events that resulted in some compromise of information or denial of service. This shows that even with a huge number of suspicious activities our robust layered security minimized the potential impact.

Likewise, we found that the number of computer virus and worm attacks on our systems continues to rise. For these attacks, our computer emergency response team has so far proven to be one of the best in the country. They provide monitoring of our networks and systems. They respond rapidly to suspicious events and are responsible for distribution of security patches and virus signatures. With the use of technology procured to support improved management of our networks and systems, we are developing better methods for obtaining patches for discovered software vulnerabilities and pushing them out to our bases. We have established a goal for implementing vulnerability patches within 24 hours of receipt. We will accomplish this goal by unwavering management focus on this important task and mandating all major commands be compliant with our Time Compliance Network Order—a process that formally tasks our units to install the patches with formal tracking of compliance.

I would like to describe to you some security policy and process successes to date. We have just finished developing the Air Force's first Cyber Security Strategy. This strategy is based on the recent National Strategy to Secure Cyber Space as well as the DoD Information Assurance Strategy. Our cyber security strategy lays a systematic framework for establishing our future information assurance policies, plans, and programs. Incorporated with that strategy is a metrics plan to enable every information assurance decision maker at every echelon to know the cyber security health of our information infrastructure.

A key element of the Air Force cyber protection capability is the DoD Common Access Card program. As of 1 March this year, 320,000 Air Force personnel have these cards. By October 2003, we plan to have over 500,000 cards issued. The cards for the remaining Air Force members will be issued in 2004. Each active duty, guard, and reserve airman will have a card as will each Air Force civilian employee and many of our contractor personnel. I recently directed that all Air Force computers be equipped to accommodate the Common Access card technology. We will use the Common Access Card to replace less secure password authentication mechanisms, to secure the physical access to our buildings, and to implement digital signatures. In addition, we are studying the potential to add biometric capabilities such as fingerprint scanning, retinal scanners and face recognition technologies to compliment the capabilities of the Common Access Card

Technical assessments and audits help us in employing the best procedures in protecting our networks. The Air Force Information Warfare Center conducts comprehensive assessments of our information assurance posture through the use of simulated hostile attacks or "Red Teaming" by our information warfare "aggressor" squadrons, Network Vulnerability Assessments, and our Air Force Information Assurance Assessment and Assistance Program visits to each of our installations. In 2002, they conducted 90 vulnerability assessments for Air Force and other DoD customers. We provide the lessons learned from these assessments to the corporate Air Force. To compliment these technical assessments, the Air Force Audit Agency conducts targeted audits to evaluate compliance with information assurance policies and directives at all echelons. In all cases, they work with our system operators and Air Staff leadership to help firm up our information assurance posture.

Our successful information assurance program is due to a dedicated and vigilant force of men and women who take pride in serving their country. These personnel in uniform, government employees, and contractor personnel are dedicated to protecting our networks and supporting our operational forces. While all of our personnel are part of our information security strategy, approximately 9,000 have significant information responsibilities. In 2002, over two-thirds of these people received specialized training. Those who could not receive traditional or computer based training learned new techniques and skills on the job. We also rely on our information system users to help in our cyber security efforts. In 2002, we provided information security awareness training to some 410,000 Air Force members and contractor personnel. The combination of a well-trained information assurance force with an informed, vigilant user community is the key to continued successful protection of the network.

### **Future Challenges**

To continue our efforts to support the expeditionary forces of the future, I see a number of opportunities and challenges ahead. One of our technology challenges is to continue to build and expand our information technology infrastructure. As I mentioned earlier, our Combat Information Transport System or CITS program is the overarching program to expand our base common infrastructure and achieve our goal of net-centricity. However, our modernization pace is slower than we like. In the near term, we need to continue the expansion under Combat Information Transport System to build out the local base infrastructure to be able to harness and use the capabilities that the GIG Bandwidth Expansion provides.

As we develop a globally based command and control system, we are developing secure communications capabilities that go across all three information domains (ground, air, and space) seamlessly enabling the warfighter to maintain information dominance. The Air Force Cryptographic Modernization program delivers critical capabilities focusing on cooperative air identification, secure anti-jam command and control to ensure positive control of nuclear weapons. The National Security Agency has identified phase-out dates for existing crypto systems and has developed a roadmap for replacement systems. This roadmap addresses the full range of modernization issues, including dated cryptography technology, changing performance parameters, and obsolescence concerns. While we have identified significant investments in the Cryptographic Modernization in the FY 04 budget, additional investments will be required in future years to avoid loss of operational capabilities as our many cryptographic systems become obsolete.

The ability to support information dominance through net centric operations demands a highly skilled and trained workforce, as users, operators and administrators. While we are aggressively training our operations and cyber security force, one of our challenges is retention of these skills in a highly competitive industrial market environment. We are identifying ways to retain these vital assets, including bonuses for some of our communications career fields. However, we are also fully open to leveraging this same industrial market environment as we evaluate commercial-like information technology functions for possible outsourcing. Our objective is to free up some of our military and civilian IT professionals to align these skilled individuals with higher priority information technology mission requirements within the Air Force. However, we are finding that our

current legal and policy framework makes outsourcing complex and that it takes far too long to accomplish simultaneously, often two to three years.

Another challenge is how to effectively manage the vast amount of information available so that we can provide the warfighter and decision maker with the right information at the right time in an assured and trusted environment. We continue to refine our strategy for providing seamless information management across the Air Force enterprise capitalizing on available commercial practices (push-pull technologies, computer data exchange standardization, common terminology and tools, and standardized formats). One element of our strategy is to clearly establish data "stewards" within our Air Force communities. The data steward will be the trusted authoritative source of data/information who will be responsible and accountable for ensuring that information is available throughout the enterprise.

As I noted earlier, we are making great strides in our information protection efforts. We are detecting and blocking literally millions of attacks against our systems each year. However, we realize that our adversaries will continue to become more sophisticated. As a result, our protection capabilities must also continue to improve. Our cyber security policies and programs must focus on both external threats as well as internal threats, both malicious and accidental.

With our desire to leverage commercial capabilities and software products, we find that we reap the consequences of the poor quality of current commercial software products. The products provided by our large commercial vendors are regularly found to have flaws that could permit compromise of our systems and interrupt our warfighting capabilities. And, these flaws are being discovered at a rate that is alarming--literally multiple flaws discovered



each day! In addition to the vulnerability presented, the cost to the Air Force to patch and fix these software systems is very large and growing. We are now spending more money to patch these systems than we pay to purchase the products. This is a national crisis and deserves the attention of our government and corporate leadership. We simply cannot afford the patch-test-find-patch again process that is the norm today. I have personally talked with software vendors about this issue, but your support could assist us in this endeavor.

In summary, our information technology and information assurance strategy, policy, plans, and programs continue to be a priority to the Air Force senior leadership. To date, we have made considerable and measurable achievements. However, we also recognize the challenges that lay ahead of us. We appreciate the support we received from Congress to date with respect to these programs, and we request your continued support.

I appreciate the opportunity to address this Subcommittee. This concludes my testimony.

NOT FOR PUBLICATION UNTIL  
RELEASED BY THE  
HOUSE ARMED  
SERVICES COMMITTEE

STATEMENT OF  
DAVID M. WENNERGREN  
DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER  
BEFORE THE  
HOUSE ARMED SERVICES COMMITTEE  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES  
SUBCOMMITTEE  
3 APRIL 2003

NOT FOR PUBLICATION UNTIL  
RELEASED BY THE  
HOUSE ARMED  
SERVICES COMMITTEE

Mr. Chairman, distinguished members of the Terrorism, Unconventional Threats and Capabilities Subcommittee, thank you for inviting me to discuss the Department of the Navy's (DON's) vision for harnessing the power of emerging technologies to equip our forces to meet the demands of the warfighting environment today and in the future.

#### TRANSFORMATIONAL VISION

As the Navy-Marine Corps team moves forward to meet the challenges of the 21<sup>st</sup> Century, our Naval Power 21 vision defines new ways of deterring conflict, new capabilities for waging war and new technologies leading to major increases in operational effectiveness. The transformation will be enabled by interoperable, net-centric operations between Joint Service, Allied and Coalition forces to defend America's interests anywhere in the world. We are building a net-centric environment, integrating the Department's information management/information technology (IM/IT) capabilities across the Sea-Air-Land-Space domain to provide improved capabilities to our warfighters.

#### NET-CENTRIC OPERATIONS

Net-Centric Operations (NCO) will link sensors, shooters and commanders to provide the superior knowledge required for a more precise, agile, and responsive style of warfare that can sustain sealane access and decisively influence events ashore anytime, anywhere. NCO will provide future warriors superior knowledge from real-time netted sensors, enabling them to act at a faster pace than an adversary.

FORCEnet is the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space, from sea to land. It is crucial to Navy and Marine Corps transformation and is the Naval vehicle to make NCO an operational reality. Through FORCEnet we will link the Navy Marine Corps Intranet (NMCI), the Department's shore-based network; Information Technology 21 (IT-21), the Navy's afloat network; the Marine Air-Ground Task Force (MAGTF) Tactical Data Network (TDN), and the Base Level Information Infrastructure (BLII) program into a seamless enterprise network that forms our contribution to the Department of Defense (DoD) vision of a "trusted, dependable and ubiquitous" network.

The NMCI initiative provides the full range of state-of-the-art network-based information services through an innovative performance-based contract using state of the market equipment and industry leading service providers. NMCI replaces numerous independent and disparate networks ashore with a single secure network and is a vital part of the DoD Global Information Grid, interfacing with IT-21 and MAGTF TDN to enhance the flow of mission critical information to forward deployed forces. NMCI significantly improves the security of our IT enterprise; increases productivity by greater sharing of knowledge and improved interoperability, and gives the Navy and Marine Corps secure, universal access to integrated voice, video and data communications.

The transformational value of this revolutionary initiative has been demonstrated repeatedly. In addition to the tragic loss of life in the September 11, 2001 attack on the Pentagon, the Navy also lost the use of almost 70% of its Pentagon office space. Through the power of a single integrated service provider, the NMCI Information Strike Force was able to reconstitute service to the Navy, replacing hardware, reestablishing the network, and putting roughly 700 people back on line in a few short days, permitting the Navy staff to resume operations in record time. The enhanced security afforded by this enterprise network was demonstrated during the recent "SQL Slammer" attacks on networks. Strictly limiting our NMCI Internet exposure to three external gateways that the Defense Information Systems Agency provides, we exercised our robust firewall policy, intrusion detection systems, filtering and Information Assurance Bulletin/Alert implementation procedures to shield our systems and not a single network or user operating within NMCI was affected by the attack.

IT-21 is a systems approach to IT investment. It brings together software applications and improved shipboard local area networks (LANs) to support embarked staffs, aviation wings, Marines and Combined Forces. It also provides increased storage and distribution at multiple levels of classification to support Joint and allied/coalition operations and satellite communications systems with enough bandwidth to transport large volumes of data into a set of end-to-end capabilities for our forces afloat. Similarly, MAGTF TDN provides network connectivity to Marine Corps Forces as they move from their sea base to their objectives and while conducting sustained operations ashore. MAGTF TDN is an expeditionary capability that provides network connectivity to all components of the

MAGTF. This connectivity includes connections to the Combined/Joint Task Force headquarters and other Service components.

The BLII program modernizes existing IT facilities and installs capability where none exists at major fleet concentration bases and stations outside the United States, providing seamless interface from these locations to NMCI, IT-21 and the rest of the Global Information Grid.

By adapting existing Naval and other Service systems and commercial products in innovative ways, we have developed systems that will be essential elements of future Joint, Inter-Agency and Coalition operations. Beginning as the Naval Fires Network, the Joint Fires Network (JFN) is an architecture that addresses the need for near real time intelligence correlation, sensor control, target generation and development, mission planning, interfaces with engagement systems, and battle damage assessment in time critical strike planning. JFN is realized by interfacing the best elements of three existing systems into a converged architecture: Joint Service Imagery Processing System-Navy (JSIPS-N), derived from a system developed by the Air Force; an adapted Army system, Tactical Exploitation System-Navy (TES-N); and the Global Command and Control System-Maritime (GCCS-M).

Navy, Coast Guard, Allied and Coalition ships form an integrated battle force in current naval operations. Communications by secure email and web services have become the de facto standard for the command and control of this type of force, providing increased



situational awareness, better logistical support and increased information sharing. Access to email and battle group web sites is essential and our Combined Enterprise Regional Information Exchange Systems (CENTRIXS) allows us to configure ship networks and conforms to DoD and NATO architecture and standards. In the past year we have equipped all deploying warships, including two high-endurance Coast Guard cutters, with CENTRIXS capability and provided the architecture to our Allies to enable them to fit out their ships.

In response to Joint requirements, Deployable Joint Command Center (DJC2) is being developed with OSD and Joint Forces Command (JFCOM) oversight. Designed to support a Joint Task Force Commander and staff, DJC2 is Joint from its inception. Using lessons learned from current diverse transportable command centers fielded by the Services and Combatant Commanders, DJC2 will be based upon known Joint or Service systems that are already mature or maturing. DJC2 will be the material piece of the Standing Joint Force Headquarters (SJFHQ) JFCOM is tasked to develop.

#### KNOWLEDGE CENTRIC INITIATIVES

As we achieve a seamless enterprise network structure, we are simultaneously transforming the way in which information is shared to truly achieve knowledge superiority. Key to the success of our knowledge management efforts is the development and use of collaborative environments and communities of practice. Commands across the Navy – Marine Corps team are leveraging the tenets of knowledge management to create virtual collaboration environments for distance learning, telemaintenance and

telemedicine. In our Collaboration at Sea project, shared information and collaborative planning and decision-making were achieved through the use of a standardized website for non-real time collaboration, chat capability for real time collaboration, and customized website replication to minimize bandwidth requirements for deployed units.

Our use of Communities of Practice has allowed us to truly make knowledge “actionable.” The Naval Education and Training Command (NETC) has structured thirteen separate learning centers and hundreds of communities of practice to enable the distributed sharing of targeted content and knowledge management. Naval facilities engineers have shared experiences and information to develop a new, more cost effective formulation for concrete used in pier building. Our submarine community at the Naval Submarine Base, Kings Bay, Georgia has initiated a collaboration and knowledge sharing initiative that will draw upon the experiences of the commands and individuals at Kings Bay to create enriched off-crew training using online, interactive and hands-on techniques.

Our goal is a web-enabled Navy-Marine Corps team, allowing our mobile workforce to have access to self-service transactions, via the web, around the world. Our movement to web services solutions will provide for the establishment of single authoritative data sources and eliminate “stand-alone” and “stove-piped” legacy systems. The cornerstone to this web-enabling effort is our development of the Navy Marine Corps Portal (NMCP). This enterprise portal will provide an integrated collaborative environment and personalized, role-tailored access to information in real time. This single integrated

portal structure will allow our organizations to focus on content delivery, and avoid the costs of individually developing portal features and functions. The NMCP will also reduce application costs, and improve information security, providing our Sailors, Marines and civilians with access to the intellectual capital of the entire Navy– Marine Corps team.

We have made significant progress in supporting the development and use of an Enterprise Architecture for the Department, and have developed policy and guidance in the areas of data, IT infrastructure, standards, applications, and warfighting and business processes. To effectively implement portfolio management, we have identified 23 Functional Areas and assigned responsibilities for managing processes, applications and databases within these areas to Functional Area Managers (FAMs). The FAMs and technical personnel are working to reduce the total number of applications used across our enterprise to eliminate redundant systems and achieve uniform standards and a consistent set of network tools throughout the Department. To date, by eliminating outdated and duplicative software, they have reduced the number of approved applications by over 89%, from 67,000 to 7,000. Our FAMs are identifying, aligning and improving business processes to maximize operational effectiveness and make sound investment decisions. Technical experts within functional areas are defining standards that will maximize information exchange through the use of the maturing commercial technology known as Extensible Markup Language, or XML. Our XML policy, which is the first published by a Federal Agency, is providing the means to facilitate data

exchange among diverse information systems, essential to establishing a net-centric environment.

## FULL DIMENSIONAL PROTECTION

The 21<sup>st</sup> Century presents new challenges for continued maritime dominance and our national security. The security of our information, systems, personnel and critical infrastructure assets is fundamental to our continued success. We have crafted an approach we call "Full Dimensional Protection." Joint Vision 2020 states that Full Dimensional Protection is achieved "through the tailored selection and application of multi-layered active and passive measures." For the Department of the Navy, that protection takes three forms: (1) protecting Knowledge pathways through Information Assurance (IA) and Defense-in-Depth, (2) protecting our Centers of Knowledge through Critical Infrastructure Protection (CIP), and (3) protecting our Knowledge Workers through efforts to protect individual privacy. These protection efforts will ensure the reliability, availability, and integrity of DON information and information systems; protect our people, and protect the critical infrastructure needed to defend and secure our mission-critical capabilities.

IA is essential for warfighting and homeland defense. It is required operationally in the Department of the Navy to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Recent denial of service and malicious code attacks; combined with the inability of any one specific defense to stop these attacks, dictate the necessity for a multifaceted,

integrated system, network security defense. The Department has adopted the defense-in-depth strategy to mitigate the risk associated with a single point of failure. Available protection technologies are employed in a layered system of defenses. To this end, attacks directed against systems within defined network boundaries are met by a series of protection mechanisms including, but not limited to, encryption, intrusion detection systems, access control, user identification and authentication, malicious content detection, audit, and physical and environmental controls. Use of these mechanisms will mitigate inherent system vulnerabilities and counter potential threats. The number and type of defense mechanisms used in each boundary layer is a consequence of the protective qualities of the device and the assigned value of the information within the protected enclave. Without appropriate information assurance, reduction or denial of information resources would have a major detrimental effect on the ability of the Navy and Marine Corps to fulfill critical operational missions.

We have established an Information Assurance Policy and are developing an overall Department of the Navy IA Strategy and a Federal Information Security Management Act (FISMA) Action Plan to ensure the Department as a whole is working together to improve and carry out effective IA programs. We are also developing policies for wireless security and remote access to information systems for our reservists and personnel away from their workplace. With these policies in place, and the development of an effective metrics system, our oversight programs will enable us to continually monitor the state of information assurance within the Department. We test the effectiveness of our information assurance posture by conducting annual assessments and

audits of information security, reviews by the Inspector General, and through Red Team operations. The Navy and Marine Corps have infrastructure and personnel in place for ensuring detection, notification, and remedial action of deficiencies and security incidents.

We have put into place an aggressive Critical Infrastructure Protection (CIP) initiative to (1) identify infrastructures, both cyber and physical, essential to warfighting readiness and achievement of operations plans; (2) assess their vulnerability to loss from terrorist actions, natural disaster, or human error; (3) develop a coordinated physical and cyber indications and warnings capability, and (4) take necessary action to ensure the achievement of Navy and Marine Corps objectives in the event of the loss of critical infrastructures.

In my role as Critical Infrastructure Assurance Officer (CIAO), I have worked with organizations across the DON to develop a plan that identifies and protects our critical infrastructure and oversees implementation efforts across the Navy and Marine Corps. A senior council guides the overall direction of this enterprise-wide effort. We have developed a groundbreaking CIP self-assessment tool and reference guide on CD-ROM that provides our base commanders with the capability to identify and assess infrastructure vulnerabilities and strengthen their critical asset protection postures. We built upon existing best practices in force protection, anti-terrorism and systems security; adding new initiatives that promote understanding of mission dependence on commercial, state and local infrastructures. This expanded vulnerability assessment process not only



identifies mission critical vulnerabilities, but also recommends appropriate corrective action.

We have partnered with state and local governments, as well as private industry in meeting CIP challenges. For example, we have pursued regional Integrated Vulnerability Assessments with Homeland Security officials. In 2002, we conducted Naval Vulnerability Assessments of the National Capitol Region and Hampton Roads area, working closely with the Secure Virginia Panel. We also conducted the first multi-jurisdictional, cross-border tabletop CIP exercise in June 2002. Entitled "Blue Cascades," the event was attended by over 150 representatives from 70 public and private sector organizations. The exercise was hosted by the Pacific Northwest Economic Region (PNWER) and cosponsored by the Navy, the Federal Emergency Management Agency (FEMA Region 10) and the Canadian Office of CIP and Emergency Preparedness (OCIEP).

Privacy is the third leg of our Full Dimensional Protection program. Now, more than ever, striking the delicate balance between personal privacy and national security is a challenge faced by the entire nation. The strengthening of security controls throughout the country has heightened America's sensitivity to the protection of civil liberties. The Department of the Navy recognizes this fact and has taken proper steps to ensure privacy protection by creating tools and policies to aid in the protection of personal information in DON systems. To support these efforts, we developed and distributed within the

Department a privacy education and awareness tool CD-ROM, and are developing a Privacy Impact Assessment for use by our program managers.

#### eBUSINESS/eGOVERNMENT INITIATIVES

Our eBusiness efforts are transforming labor-intensive paper processes into reengineered, efficient, and effective web-based solutions. Aligning with the tenets of the President's Management Agenda, our efforts have achieved, and will continue to produce, substantial efficiencies and significant resource savings and cost avoidance across every mission area of the Department – providing the force multipliers of value and improved services to the warfighter. We established the DON eBusiness Operations Office as an innovation center to encourage commands to adopt eGovernment solutions. The efforts of this office, in particular its pilot initiatives, have resulted in significant achievements. For example, a \$100K investment in a web-based medical appointment initiative at the Naval Medical Center, San Diego will eventually yield a cost avoidance for DoD of about \$18M and provides markedly improved customer service. The DON received a 2002 eGovernment Performance Leader Award for this initiative.

I chair the DoD Smart Card Senior Coordinating Group (SCSCG), a DoD-wide alliance for rollout of a single smart card across the Department of Defense. The result of this group's efforts is the successful rollout of the Common Access Card (CAC) that is being issued to all active duty military, Selected Reserve, government civilian and selected contractor personnel – a total population of approximately four million. It serves as the new Geneva Convention identification card for military members and is our cyber

identification and physical access card. To date, the DoD has issued over 2.2 million CACs and the DON has been a leader in this effort with over 890,000 CACs issued to Navy and Marine Corps personnel. The value of the CAC is multi-dimensional, but one of its greatest attributes is as the carrier of our Public Key Infrastructure (PKI) digital certificates, providing the ability for cryptographic logon to networks, secure authentication to protected websites and the ability to digitally sign electronic transactions, which are key to the success of our eGovernment transformation. We will continue to expand and improve the Common Access Card, and are currently developing and testing the next generation CAC platform that will incorporate contactless and biometric technologies to further enhance and strengthen our physical security and force protection efforts.

#### IM/IT WORKFORCE

People are the heart of our organization. We know our real power comes through our people - what they know, how they bring their knowledge together and how they translate that knowledge into action. As a result, we are always looking for ways to provide our personnel with opportunities to develop professional skills aligned to mission requirements. We are identifying specific ways to recruit and develop employees who have the knowledge, skills, abilities and behaviors needed to support current and emerging mission requirements; and are strongly committed to provide both our military and civilian IM/IT personnel the opportunities they need to stay current in an increasingly complex technology-based environment. To meet our people's career development needs, and thereby achieve our broader goal of a highly skilled workforce, we have been

developing guidance, tools, and programs that focus on career development. As an example, the establishment of the Navy Information Professional officer community assures the growth and development of individuals who will be critical to our IT future.

Under the Information Assurance (IA) Scholarship Program, we have provided graduate level IA education to Navy and Marine Corps personnel serving in critical security billets. To ensure our Sailors returning from sea duty keep their skills current, we are capitalizing on the training opportunities afforded by NMCI, assigning them to work in our network operations centers alongside -- and training with -- our support contractors in a world class environment. For civilians, we have defined the competencies that we believe are key to our future and provided a tool for career planning. The Federal CIO Council has adapted the tool for use across the Federal Government as the IT Roadmap career development tool for over 66,000 IT professionals. Given the diverse challenges that we continue to face, we recognize that we must stay vigilant to the needs of our people, which will continue to evolve and require resourcing to enable us to stay responsive to mission requirements.

#### DON IM/IT GOVERNANCE

We have embarked upon a significant restructuring of information management/information technology governance across the Department. This restructuring will strengthen, align, and integrate our IM/IT efforts across the Navy and Marine Corps; strengthen the tie between the Secretariat and the Services; and ensure Department-wide alignment of IM/IT efforts with warfighter priorities. A key element of

the restructuring was the designation of RADM Thomas E. Zelibor, Director, Space, Information Warfare, Command and Control Division (CNO N61) to be dual hatted as the Department of the Navy Deputy Chief Information Officer (Navy) and BGEN John R. Thomas, Director for Command, Control, Communications, and Computers (C4) to be dual hatted as the Department of the Navy Deputy Chief Information Officer (Marine Corps). These designations as DON Deputy CIOs are in addition to their C4 responsibilities in the operational chain of command and are separate and distinct from their CIO responsibilities. However, this dual hatted organizational structure enables a close alignment between C4 and CIO responsibilities. Another essential element of the restructuring is the development of a DON IM/IT Enterprise Implementation Plan. This plan will link our vision and strategy to programmatic and budgeting guidance and serve as the basis for approving and funding IM/IT investments.

Mr. Chairman, members of the Subcommittee, I thank you again for allowing me the opportunity to speak to you today. We greatly appreciate your support of our information technology initiatives to meet the challenges we face and I look forward to working with you on these important initiatives.

I will gladly answer any questions that you may have about the Department of the Navy's information management/information technology initiatives.

NOT FOR PUBLICATION  
UNTIL RELEASED BY  
THE HOUSE ARMED  
SERVICES COMMITTEE

STATEMENT OF

BRIGADIER GENERAL JOHN R. THOMAS

DEPARTMENT OF THE NAVY

DEPUTY CIO FOR USMC

AND

DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS

HEADQUARTERS, UNITED STATES MARINE CORPS

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS

AND CAPABILITIES SUBCOMMITTEE

ON

APRIL 3, 2003

CONCERNING

DEPARTMENT OF DEFENSE FISCAL YEAR 2004

INFORMATION TECHNOLOGY POLICY AND PROGRAMS

NOT FOR PUBLICATION  
UNTIL RELEASED BY  
THE HOUSE ARMED  
SERVICES COMMITTEE



**Brigadier General****John R. Thomas**

Director for Command, Control, Communications, and Computers (C4), and Chief Information Officer (CIO) for the Marine Corps



Brigadier General Thomas is the Director for Command, Control, Communications, and Computers (C4) for the United States Marine Corps, the Chief Information Officer (CIO) of the Marine Corps and Commander of the Marine Corps component to the Joint Task Force for Computer Network Operations.

Brigadier General Thomas was commissioned a second lieutenant in May 1973. He is a graduate of Appalachian State University with a Bachelor of Science Degree, Prairie View A&M University with a Master in Business Administration, and Naval War College with a Master of Science in National Security and Strategic Studies. His military schools include the Basic School, Advanced Communications Officer School, United States Marine Corps Command and Staff College, and the College of Naval Warfare.

His previous command assignments include:

- Commanding Officer, 1st Surveillance, Reconnaissance, and Intelligence Group, I Marine Expeditionary Force
- Commanding Officer, 7th Communications Battalion, III Marine Expeditionary Force
- Commanding Officer, Communications Company, 3d Force Service Support Group
- Platoon Commander

His previous staff assignments include:

- Deputy Director, Command, Control, Communications, and Computers HQMC
- Director, Programs Division, Programs and Resources Department HQMC
- Assistant Chief of Staff G-6, Marine Forces Pacific
- Assistant Chief of Staff G-6, First Marine Expeditionary Force
- Chief, Command Centers Support Division, Command, Control, Communications & Computers Directorate (J6), Joint Staff
- Communications Support Officer, National Military Command Center
- Program Coordinator, Space, Command and Control Directorate, Chief of Naval Operations
- Marine Officer Instructor, Prairie View A&M University

Brigadier General Thomas' awards include: Legion of Merit, Defense Superior Service Medal, Meritorious Service Medal with gold star, Navy and Marine Corps Commendation Medal with gold star, National Defense Service Medal with two bronze stars, and Humanitarian Service Medal.

Mr. Chairman and members of the Terrorism, Unconventional Threats and Capabilities Subcommittee, thank you for this opportunity to appear before the committee to discuss how the Marine Corps is meeting the challenge of providing information technology (IT) to our forces in the 21<sup>st</sup> Century.

## I. INTRODUCTION

The Navy-Marine Corps Team continues to play a vital role in protecting our American interest by participating in the establishment of stability and security in many of the world's trouble areas. Naval Forces, both Active and Reserve, are operating around the world in diverse locations, from Afghanistan, the Horn of Africa, and Southwest Asia. The unique and powerful capabilities that the Naval Services bring to our joint forces are key elements of our Nation's military power. Marine Corps operations throughout the past year have highlighted the versatility and expeditionary nature of our forces. Today, nearly two-thirds of our Command, Control, Communications, and Computers (C4) assets are deployed in support of ongoing operations. C4 is crucial to the success of Naval Forces in the 21<sup>st</sup> century.

Access to information across and external to the five elements of the Marine Air Ground Task Force (MAGTF) is becoming the lifeblood for full spectrum dominance of deployed Marine units and is the basis for C4 transformation. The days are rapidly fading when hand and arm signals and single-channel radio alone will suffice as the primary means of communications for commanders and support personnel. Operational concepts like Expeditionary Maneuver Warfare (EMW) and Sea Basing drive the need to access and exploit the power of global networks to support decision-making. The opportunity to exploit this new "digital dimension" of the battlefield, once enjoyed mainly by those in senior headquarters, now must extend down to the last tactical mile. Assured access to "the network" is key to successful warfighting. The challenge for the Marine Corps is to enable this access to every element of the MAGTF. To support command and control, IT systems must integrate information capabilities across a range of functional areas while supporting a constantly changing environment. Expeditionary commanders, regardless of their location, must have the ability to securely and rapidly access and transfer voice, video, data, and imagery information. To do that requires

integrated, robust, secure, and interoperable information systems and networks. As a result, the Marine Corps' has initiated C4 programs, many of which are addressed in this budget, which will further transform our Corps.

## **II. THE BASIS FOR CHANGE**

The Marine Corps approach for net-centric operations begins and ends with the individual Marine aided by a seamless, end-to-end, meshed network comprised of sensors, Command and Control (C2) nodes, and weapons platforms.

Our expeditionary ethos demands proficiency in net-centric operations that combine planning, enhanced situational awareness (SA), and decentralized decision-making through secure, flexible, redundant, tailored, and assured information flow. Information technology (IT) will support new relationships on the battlefield among intelligence, surveillance, and reconnaissance (ISR) sensors; C2 nodes; and weapons platforms. By exploiting new technologies (e.g. Web), and improving and maintaining a robust C4 infrastructure, we enable increased information flow and the ability to increase the tempo of operations. C4 networks are no longer pipes simply delivering information. Rather, they are the catalysts for speed of command and process change, enabling an enhanced focus to achieve the desired effects of military operations. They also reduce forward deployed footprints. Receiving engagement quality information from ISR assets and providing it to weapons platforms requires common, shared, SA from commanders and staffs to individual Marines. I will highlight those programs and initiatives that allow us to build, defend, and exploit the network.

## **III. BUILD THE NETWORK**

The Marine Corps is meeting the challenge of net-centric warfare through a combination of initiatives that are essential to building this integrated network capability. The most important element in the equation is the individual Marine and "civilian Marine" who are motivated, well trained, and educated on the operational as well as the technical employment of advanced C4 systems and networks. We are working hard to recruit, train, and retain our C4 Marines and civilians. To accomplish this goal, we have restructured the unrestricted C4 officer Military Occupational Specialty (MOS) to ensure

the right grades, skills, and numbers are at the right unit level. We have instituted a career management program for our IT civilians. C4 Warrant Officer Training has been consolidated at the Command and Control Systems School at Quantico, VA. Similarly, we have reorganized and expanded our enlisted MOS and the associated training at the Marine Corps Communications Electronics School at Twenty-nine Palms, CA. in order to remain relevant to current and emerging technologies particularly in the area of networking. We are working equally hard to retain our Marines through the application of reenlistment bonuses and education opportunities in programs like Naval Postgraduate School. The Marine Corps is also participating in the Information Assurance Scholarship Program (IASP) as an avenue to qualify Marines as Information Assurance Technicians. In a precedent setting initiative, Marine Staff Non Commissioned Officers (SNCOs) are attending the Air Force Institute of Technology for advanced education with follow on assignments in their new MOS to senior level Marine Commands to provide staff support for Information Assurance. As we invest time and resources to train our smartest personnel, we must also provide an environment that encourages retention and career progression for Marines and civilian Marines alike. At the same time, commanders and their staffs require increased training opportunities to effectively exploit the information provided in net-centric environments and to speed the pace of information. Training for staffs in C2 becomes more critical as more transformational concepts are developed that provide increased reliability, accuracy, and speed of information for decision-making. Technology provides incredible opportunities for the future, but our greatest resource will always be the Marines who make it work.

To transform today's legacy networks requires persistent IT governance, and adherence to an open systems joint enterprise architecture with well defined data standards. Working in close coordination with the Office of the Secretary of Defense, Department of the Navy Chief Information Officer (CIO), the Joint Staff, and Services, we are committed to the preparation of this *enterprise* IT architecture that is integrated into the Global Information Grid (GIG).

The Marine Corps Enterprise Network (MCEN) is our contribution to FORCEnet. The MCEN consists of a globally interconnected, end-to-end set of information

capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand. It is the Marine Corps segment of the Global Information Grid (GIG). Programmed enhancements to MCEN will provide a significant contribution to FORCENet and the GIG. MCEN supports all data and information exchange requirements for Marine Forces worldwide; the MCEN consists of the Navy Marine Corps Intranet (NMCI), Information Technology-21, and the MAGTF Tactical Data Network (TDN). To enhance MCEN performance and reduce cost, we instituted a process to substantially reduce the number of legacy applications on the network from nearly 7000 to 500. Also, we are working to create a shared data environment that will provide further data standardization thus increasing interoperability for our IT capabilities. Finally, we stood up a governing body, the Information Technology Steering Group (ITSG) chaired by the CIO and is comprised of representatives from each element of the MAGTF and principle organizations (e.g. Marine Corps Combat Development Command, Marine Corps Systems Command, Programs and Resources Department). The ITSG makes recommendations to the CIO relative to implementation across the MAGTF. This ensures a disciplined and enterprise approach to provisioning and deploying information technology. From this, the Marine Corps gains economic efficiency and a high degree of integration and system interoperability.

**Navy-Marine Corps Intranet (NMCI).** We have eagerly anticipated the implementation of NMCI services since contract award in October 2000; Electronic Data System (EDS) assumed responsibility (AOR) for the first 7,100 (of 89,400) Marine Corps users on 24 March at Quantico, VA. The Marine Corps will transition to NMCI throughout FY03 and into FY04. We have a FY06 Military Construction project to build a Network Operation Center (NOC) planned for Quantico, VA. We are continuing to refine the overall cost of NMCI. For example, the demand for NMCI-like services has increased significantly post-9/11. The Marine Corps remains committed to the overall goal of a single DoN enterprise network, and to NMCI as the means to achieve that goal; however, accurately planning for the transition of forces supporting Operation Enduring Freedom, Iraqi Freedom, and the Global War on Terrorism remains a challenge and may impact the transition schedule. We are working hard to avoid actions that negatively

impact readiness, and are working closely with Director NMCI and his staff on the various challenges associated with transitioning the Marine Corps and the Navy to NMCI. The cooperation on the program between the Government and EDS remains strong.

Enhanced capabilities, offered through new systems fielding will allow us to build the deployed network to meet the demands of warfighters in network-centric operations. "Power to the edge" and empowering users requires moving bandwidth to the edge. We have taken action to increase the bandwidth available at the group and regimental levels with wideband satellite communications systems. To improve our tactical flexibility and strategic agility, we must ensure our communications packages support a wide range of missions over greater distances. This requires an increase in available satellite terminals providing the necessary reach and ability to conduct distributed operations throughout the battlespace beyond the littorals, while remaining connected to MAGTF, naval, joint, and national security systems. Marine forces operating beyond line of sight must be able to connect via airborne relay provided by unmanned aerial vehicles, MV-22s, and satellite links to seabased forces, and be able to reach back to supporting elements for C2, SA, and sustainment information. The resultant shared data for air, ground, combat service support, and command elements of the MAGTF will create a powerful synergy for transformation.

The ability to connect through satellite communications enabled Marine Corps forces in Afghanistan, operating well beyond the littorals, to provide communications for C2, intelligence, and logistical support. Marines were able to reach back to the Supporting Establishment from forward operating locations by connecting to the Defense Information Systems Network and selected intelligence networks. This strategic agility to operate deep in Afghanistan was provided by the well-trained Marines of the joint task force enabler package, a forerunner of the First-In Command and Control System.

**Joint Tactical Radio System (JTRS).** Revolutionary in its effect on MAGTF warfighting capabilities will be the fielding of the JTRS. The purpose of the JTRS program is to develop a single, interoperable, joint radio that will provide a secure, software-programmable, multiband, wideband mobile network backbone. JTRS promises



to provide wide area network access and increased information exchange capabilities down to the last tactical mile and out to the forward edge of the battlespace. Soon with your help we will be able to link Marines on the forward edge with those providing homeland defense with the voice capability through a networked mobile radio.

**Land Mobile Radios (LMR).** We seek greater interoperability through narrow band, secure LMR for our first responders that can interoperate with the JTRS radios we use in the operating forces.

The promise of voice over Internet Protocol (IP) reduces our forward deployed infrastructure and enhances the commonality of our networks. Our Transition Switch Module (TSM), that will replace the aging Unit Level Circuit Switch (ULCS), will position Marine forces to achieve even greater ability to use and leverage information technology to provide voice connectivity through the Defense Information Systems Network (DISN).

The increased demands and dependency on the network will require an improved means to plan, manage and maintain operational awareness of the network. The Joint Network Management System (JNMS) will provide state of the art tools and capabilities to optimize information flow to IT personnel who provide the MAGTF Tactical Data Network (TDN) and connectivity to the DISN.

**Tactical Data Network (TDN).** The TDN (comprised of HMMWV-- mounted gateways and transit-cased data distribution systems) and its sister component, the Digital Technical Control (DTC), are being fielded now throughout the Marine Corps. These systems of interconnected gateways, routers, and servers provide Secure and Nonsecure Internet Protocol Router Networks (SIPRNET and NIPRNET) from the major subordinate commands down to battalion level and form the backbone of the MAGTF TDN. TDN as with any other IT capability requires periodic refresh to keep pace with Moore's Law predictions of increases and advances in technology every 18 months.

**Lightweight Multiband Satellite Terminals (LMST).** At the regiments, air groups, and combat service support elements, TDN will connect via enhanced wideband satellite capability in the Marine Corps. The fielding of new LMSTs to the communications battalions will augment legacy ground mobile forces satellite terminals.

Continued LMST fielding to our aviation elements, together with the fielding of the Global Broadcast System (GBS) to Marine Regiments represents a revolutionary increase in wideband satellite connectivity for MAGTFs. Together with the Extremely High Frequency (EHF) capability of Secure Mobile Anti-jam Reliable Tactical Terminal (SMART-T), they will provide the commanders of all elements of the MAGTF with reliable satellite communications to joint and multinational units within a given theater or as reachback to national assets and resources such as intelligence and sustainment information. Importantly, the fielding of more and greater capabilities to major subordinate commands has allowed a shifting of assets in order to provide increased wideband connectivity to the outer edge of the MAGTF. These space-based systems, when networked with terrestrial multichannel systems, will create a robust, reliable, wideband network to support multiple commanders across a wide geographic area. Wideband terrestrial systems, once critical for connectivity at higher levels, may now be redistributed to the forward edge of the network. By leveraging existing capabilities we will more quickly realize the effects of network centric operations. The Marine Corps is, in effect, building a digital tactical internet interoperable and fully integrated into the Global Information Grid.

#### **IV. EXPLOIT THE NETWORK**

The Commandant believes that in order to achieve maximum relevance to the Nation and combatant commanders, our tactical capability must be inherently joint. The Marine Corps procures systems and employs the MAGTF in a way that demands joint interoperability, but the Commandant has further stressed this need by directing that Marine Corps capabilities will be absolutely committed to joint interoperability. We are committed to the Transformational Communications (TC) effort that envisions a Net Centric infosphere, where the Joint Tactical Radio System (JTRS), TC, GIG-Bandwidth Expansion, and Horizontal Fusion enable information flow across the enterprise resulting in a Joint force that is capable of information dominance, providing improved sense/decide/shoot cycles. Providing information to decisionmakers takes more than bandwidth and a network. It takes the ability to package and exploit the information so Marines can use their training and intuition to translate it into knowledge. The Marine

Corps intends to field a family of systems specifically designed to improve horizontal integration by standardizing capabilities within the MAGTF to translate information into knowledge.

**Deployable Joint Command and Control Capability (DJC2).** DJC2 will provide an interoperable, standardized, C4 baseline capability for future Standing Joint Task Force (JTF) Headquarters. The Marine Corps is heavily engaged in the DJC2 design effort and will be providing the Deputy Program manager.

**Unit Operations Center (UOC).** The UOC is designed to add commonality and consistency, as well as state-of-the-art technology, to the combat operations centers from the battalion to the Marine Expeditionary Force (MEF) headquarters. Designed with modular and scalable technology, the UOC will provide commanders with user-friendly consoles and displays to receive, assimilate, and display friendly and enemy data to aid in the decisionmaking process. UOC will host such applications as the global command and control system (GCCS), Tactical Combat Operations (TCO), the Advanced Field Artillery Tactical Data System (AFATDS), and the Intelligence Analysis System (IAS) as well as other key C2 and logistics systems. By providing common suites at each level of command, commanders and staffs can more readily share information and gain a common tactical picture of the battlespace.

**Common Aviation Command and Control System (CAC2S).** CAC2S will provide the means for translating the MAGTF commander's intent into aviation-specific C2 capabilities. It integrates aviation functions in air defense, air support, air traffic control, and command center operations and planning. Capable of supporting any operational contingency, CAC2S workstations incorporate common messaging, database, network, security, and display services in support of joint automated aviation planning, SA, decision aid, and tactical air operations to effectively command, control, and coordinate air operations in a joint and coalition environment. The CAC2S system incorporates the jointly mandated modules of the theater battle management core system, the system that plans, develops, promulgates, and executes the air tasking order and accomplishes the Marine Air Command and Control System (MACCS) missions with a

suite of operationally scalable modules tied to the MACCS organic sensors and weapon systems.

**Global Combat Support System–Marine Corps (GCSS-MC).** GCSS-MC provides a single focused effort to reduce overlaps in the capabilities of currently fielded Government Off-the-Shelf logistics IT systems by streamlining our IT footprint through divestiture strategies, portfolio management, and establishment of a shared data environment. GCSS-MC is the enterprise wide portfolio of Marine Corps logistics and combat service support information technology capabilities supporting a Common Logistics Command and Control System. It represents a secure, web based combat support family of systems based on interoperability and horizontal connectivity across combat support functions. By eliminating “stove piped” IT systems and delivering a robust configuration of COTS/GOTS products, GCSS-MC provides for logistics IT modernization for Marine Corps Combat Service Support planners and operators.

**Enhanced Position Location Reporting System (EPLRS).** Within our ground elements we are fielding EPLRS, a digital data radio, and the two Data Automated Communications Terminal (DACT) variants, the first a ruggedized, hand-held personal digital assistant, and the second a mounted ruggedized laptop both equipped with digital mapping, Global Positioning System (GPS), and preformatted messaging. These systems provide tactical SA from the infantry platoon level up through the Ground Combat Element headquarters.

**Data Automated Communications Terminal (DACT) / Defense Advanced Global Positioning System Receiver (DAGR).** The embedded GPS capability in the DACT will connect via the Tactical Data Network and will allow for increased SA all the way to the edge at never before possible company and platoon level. Exploiting a commander's ability to rapidly receive information from networked sensors and systems and deliver it to frontline weapons and individual Marines using the network as a force multiplier is the very essence of the transformational capability provided by the Marine Components of FORCEnet. The DAGR will support individual unit maneuver without requiring netted connectivity.

## V. CONNECTING THE NAVAL FORCE

The Marine Corps C4 department is working closely with the Navy to assist and capitalize on Information Technology 21 (IT-21) efforts. IT 21 and the Marine Corps Enterprise Network (MCEN) form the basis for development of naval FORCEnet capabilities. FORCEnet is the operational construct and architectural framework for naval warfare in the information age.

FORCEnet seeks to transform information into combat power by significantly increasing combat capabilities through the initial alignment and integration of existing networks and command and control systems. In the longer term, this process will provide for the transformation of situational awareness for all Naval forces, will accelerate the speed of decision process and allow for the effects of mass without the need to mass forces. FORCEnet seeks to capitalize on innovation, enhance experimentation, and insert emerging technology to increase the ability of Naval Forces to succeed. IT-21 systems encompass the majority of shipboard C4ISR capabilities, including SIPRNET, NIPRNET, GCCS-maritime, and super high-frequency (SHF) and EHF satellite communications, to name a few. Synchronizing C4 system installations on amphibious ships with the fielding of complementary Marine ground C4 systems is the first step to achieving naval network-centric operations. Programmed improvements in high-frequency automatic link establishment aboard amphibious ships will significantly increase the access of the deployed commander to the network and will provide greater capability to the lowest levels of the MAGTF in sensor-to-- shooter environments. The Navy-Marine Team has also made considerable progress at identifying requirements and resources to install a ship-to-shore EPLRS network. The EPLRS data radio aboard ship, completely interoperable with the EPLRS fielded to Marine infantry regiments and battalions, is the interim solution for providing the landing force with an Internet protocol network to pass data to the ship while transitioning from ship to shore. These efforts complement the ongoing coordination with the Navy on installation and configuration of wideband SHF and EHF satellite communications (SatCom) on amphibious ships. The fielding of EHF SatCom systems to both the Navy and Marine Corps offers considerable improvement to our capability to establish wideband connectivity from ship to shore.

Recent process and procedural improvements in the requirements and acquisition processes along with improvements in IT management and CIO oversight enable us to move in the direction of a common MAGTF IT environment. This will provide us with a single integrated data structure providing common element attributes regardless of the application used, common user interfaces with access to required operational functions regardless of MAGTF component or the echelon of command and interoperable applications. The result is modular mission functionality through a shared data concept that leverages virtual relational databases and displays information via a common command interface providing the basis for the seamless integration of the Marine Corps into joint network centric operations.

## **VI. DEFEND THE NETWORK**

Our centralized policy, directives, and provisioning establishes a strong baseline for Information Assurance (IA). The goals of the Marine Corps IA program include confidentiality, integrity, availability, authentication, and non-repudiation of information transported along the Marine Corps Enterprise Network (MCEN).

In concert with the other Services in support of the Combatant Commanders, the Marine Corps will achieve interoperability within the security guidelines of the new DoD IA policy. Concurrently we are revising directives that govern the Marine Corps IA program and attendant responsibilities for protecting critical processes that depend on information technologies. In addition to implementing DoD directives, the intent of our efforts is to provide an affordable IA capability that supports a robust infrastructure-wide defense in depth. In addition, as part of the development and acquisition process, the CIO validates IA operational requirements to ensure they are incorporated into all our architectures and systems.

The Marine Corps' specific objective for achieving Information Assurance is to employ state-of-the-art technology, provide awareness training to all users, and to deploy computer network defense tools across the enterprise. This is achieved by deploying a defense in depth strategy integrating the capabilities of educated users, trained personnel, proven procedures and the correct technology to achieve strong effective, multi-layer and multi-dimensional protection.



The Marine Corps' Information Technology Network Operations Center (MITNOC), located aboard MCB Quantico, Virginia, is the nerve center for the central operational direction and defense of our enterprise network. In recognition of the importance of the support the MCEN provides to our forces, the Commandant has redesignated the unit to Marine Corps Network Operations and Security Command (MCNOSC) effective 1 July 2003. This new command will have a major oversight responsibility under NMCI.

The Marine Corps exists to fight and win on the battlefield. Therefore, our operating forces are equipped with the same IA and Computer Network Defense (CND) capabilities for the tactical and deployed environments as they have in the supporting establishment. The Marine Corps fielded the Deployed Security Interdiction Device (DSID). The DSID consists of a suite of equipment that includes the same CND technologies that are found at our supporting establishment connection points to external networks. DSIDs have been distributed throughout the Marine Corps and provide our operating forces with a CND capability that they can take with them to any corner of the globe. DSID are proving their worth with current deployed forces. The DSID successfully provides computer network defense for joint service operations within USCENTCOM's theater of operations. As the Marine Corps migrates toward the Navy Marine Corps Intranet (NMCI), we are engaged with Electronic Data Systems (EDS) and their Information Strike Force (ISF) to ensure the existing end-to-end IA capability is matched or exceeded under the NMCI concept of operations.

We have made great strides in the execution of our Information Assurance Program. The "pearl" of those accomplishments is the Marine Corps' computer network defense capability. Information Assurance, however, is a continuous journey, not a destination, and to that end, our journey continues.

## **VII. CONCLUSION**

The changes, represented by the C4 network and systems described above provide the means for the MAGTF to fight and win. The Marine Corps is building the network to make net-centric warfare a reality. Your continued unwavering support of our IT

programs will provide a strong foundation on which we can continue building on our successes.



---

---

**DOCUMENTS SUBMITTED FOR THE RECORD**

APRIL 3, 2003

---

---





# Transforming to Meet the Challenges of National Defense

---

Lt Gen Harry Raduege  
Director, Defense Information Systems Agency  
3 April 2003





# Transformation: Core and Best Fit Missions

## DISA CORE & BEST FIT MISSIONS

### QDR GOALS

- Protect Critical Bases of Operations
- Conduct Information Operations
- Project Power in Denied Areas
- Deny Enemies Sanctuary
- Enhance Space Operations
- Leverage Information Technology

### CORE: Joint C4 Missions:

- Communications
- Command & Control
- Joint Interoperability Support
- Defensive Information Operations
- Combat Support Computing

White House Support

Defense Technical Information Center

Electronic Commerce & Business

Enterprise Acquisition Services

*"We need to find new ways to deter new adversaries. We need to make the leap into the information age, which is the critical foundation of our transformation efforts." - Secretary Rumsfeld*





# Global Communications

## DISN: Backbone of the GIG

### Capabilities

- Classified and unclassified
  - Voice
  - Data
  - Video
  - Imagery
  - Conferencing

### Military Value-Added Features

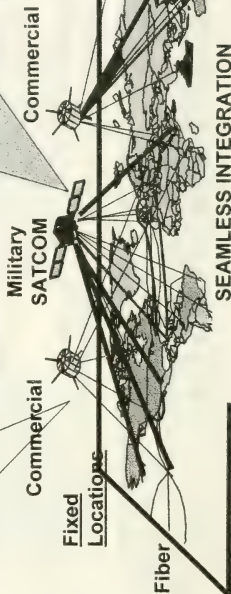
- Global reach
- Tactical extension
- Defensive IO
- Personnel & Physical Security
- Diversity & Precedence
- Visible assets
- Military Exploitation
- Interoperability

Focus on end-to-end capability and increased capacity

GIG Bandwidth Expansion

DoD Teleport

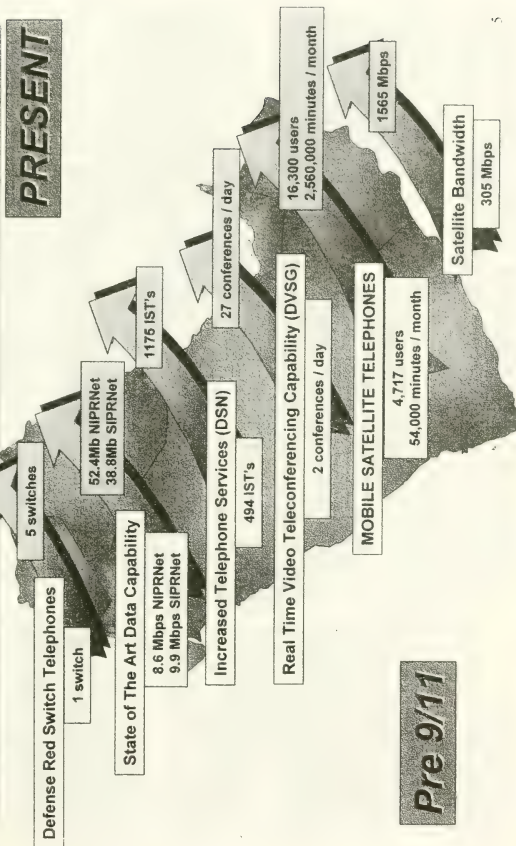
Enhanced Mobile Satellite Services





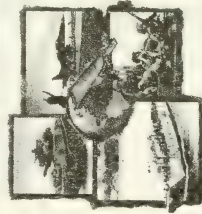
# DISN SERVICES

## Support to the Warfighter

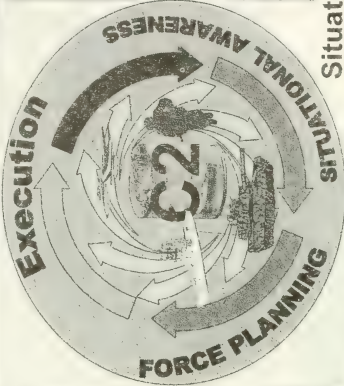


# Joint Command and Control

Global Command and Control System  
Global Combat Support System, & Defense Message System



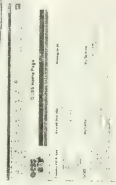
Force Planning



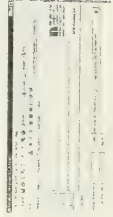
Intelligence



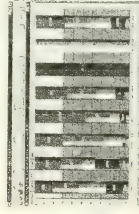
Situational Awareness



Combat Support



Messaging



Force Readiness



# Joint Interoperability Support: Executing the Mission

## Promoting Joint and Coalition Interoperability

- Support to contingencies and exercises, including "fly-away" teams
- Establishing DoD standards
- Evaluating and adopting commercial standards
- Optimizing networks for combatant commands
- Interoperability certification authority
- Spectrum management and deconfliction
- Hazards of electromagnetic radiation and ordnance analysis
- Spectrum defense
- Numerous tools to support interoperability and spectrum deconfliction

Interoperability  
= capability on  
the battlefield



# Defensive Information Operations



## JTF-Computer Network Operations (JTF-CNO)

- Reports to USSTRATCOM
- Operationalize CND & CNA
- Synchronized with air, land, sea and space forces



## Global Network Operations Security Center (GNOSC)

- Global Situational Awareness
- GIG Management
- Intrusion Detection



## Responds

## Controls

Carnegie Mellon  
Software Engineering Institute  
CERT Coordination Center

## Industry Partners Dissemination

### Nat'l Coord Center (NCC)

- Government-Industry Coordination
- NS/EP Telecom
- ISAC
- Watch Officer Visibility



## Analyzes

### DoD Computer Emergency Response Team (CERT)

- Intrusion Analysis
- Vulnerability Alerts (IAVA)
- Incident Response



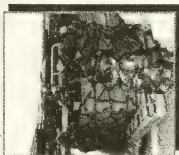


# Combat Support Computing

## DISA runs the IT systems that . . .



**provide command  
and control**



**manage parts and  
replenish supplies**



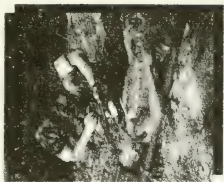
**provision ships**



**manage transportation**



**pay the warfighters**



**provide  
medical care**

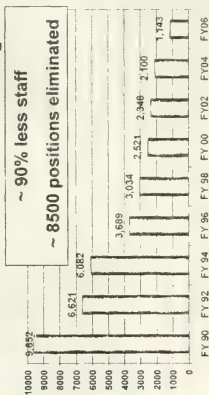


**manage maintenance**

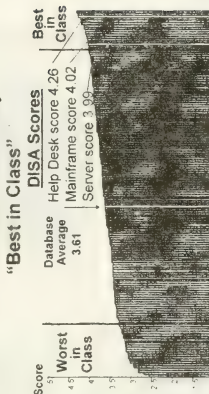


# Combat Support Computing Transformation Results

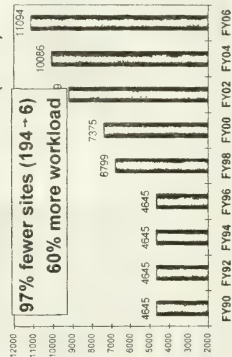
## Government Personnel End Strength



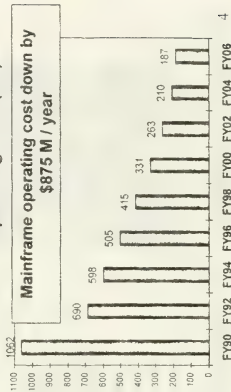
## Gartner Customer Survey



## Mainframe Workload (MIPS)



## Mainframe Operating Cost (\$M)





# Additional Responsibilities

## White House

### Communications Agency



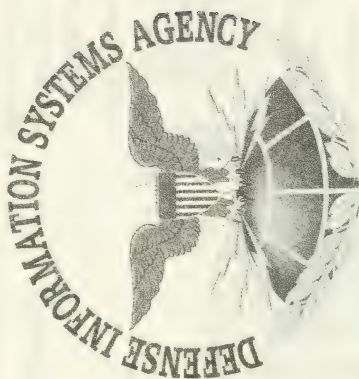
- ✓ Anywhere
- ✓ Anytime
- ✓ By any means
- ✓ Under any conditions
- ✓ To any one

## Defense Technical Information Center

- Central repository for defense acquisition, scientific & technical information
- IT support to OSD staff, Joint Staff and Service secretaries
- Classified & unclassified

## eBusiness Applications Division

- On-line solicitations
- Paperless contracting
- Central Contractor registration
- Enterprise Acquisition Services
- Shortened lead times
- Military requirements, standards, and security
- Buying power
- Administratively efficient



Global Let-Centrie Solutions - The Warfighter's Edge

---

---

**QUESTIONS AND ANSWERS SUBMITTED FOR THE  
RECORD**

MARCH 13, 2003

---

---





## QUESTIONS SUBMITTED BY MR. MEEHAN

Mr. MEEHAN. Some of the programs you've mentioned are long-term propositions, e.g., the Transformational Communications Satellite (TSAT) Program. What do you have planned in the information technology area that will benefit the warfighter and improve defense operations in the near-to-mid term?

Secretary STENBIT. In the near term, we completed launching the last of both our Milstar and Defense Satellite Communications Systems (DSCS) spacecraft, and these are currently providing operational capability to the warfighters. Both systems include significant improvements in support to tactically deployed users over the earlier versions.

In the mid-term, we are moving towards the first launch of two new communications systems. The first, Wideband Gapfiller System (WGS), is a follow-on to both the DSCS system and the Global Broadcasting System (GBS) currently hosted on another satellite. It will provide over 2 gigabites per second per satellite of lightly-protected capability, mostly to deployed users. First launch is anticipated in mid-2005. The second system, Advanced EHF (AEHF), is a follow-on to the Milstar program and will provide protected satellite communications capabilities to warfighters at much higher data rates than Milstar. AEHF first launch is anticipated in early 2007. Finally, we have a new narrowband system in development called the Mobile User Objective System (MUOS), which will support voice and low-rate data communications to users with hand-held terminals, resembling large cell phones.

We are also investing considerable effort into upgrading terminals to support higher data rates while being more mobile, and into improving our satellite control centers to be more responsive to dynamic user requirements, more efficient with resources, and better connected to the sources of information that the warfighters need.

Mr. MEEHAN. Will your Transformational Communications Satellite program enhance the Department's IT capabilities or is it a competitor for IT funds?

Secretary STENBIT. The Transformational Communications Satellite (TSAT) program is an integral part of the Department's IT capabilities. Our overall goal has been to remove communications bandwidth as a constraint to the warfighter, to the largest extent possible. TSAT is envisioned as both a space-based communications backbone, and as the beyond-line-of-sight extension of our fiber-optics and line-of-sight communications systems supporting our deployed users. We have always planned on the TSAT system as simply being one piece of an integrated IT whole, with other key components being the GIG bandwidth expansion effort and the Joint Tactical Radio System (JTRS). Commonality and interoperability between these IT components is in fact exactly what is driving us to a universal, packet-based (IPv6) approach to all communications.

The TSAT program is not a competitor for IT funds. TSAT can be said to be competing for funding with the non-transformational Advanced EHF program. By this we mean that if the TSAT program is not able to reduce risk and mature applicable primary technologies to the appropriate level (or use already mature fallback technologies), then TSAT funding may be shifted to support the acquisition of additional AEHF spacecraft. We expect that our evolutionary acquisition strategy for TSAT will be successful and allow us to deliver an initial Increment 1 TSAT that is much more capable than AEHF and therefore start the DoD SATCOM program down the transformational path to netcentric operations capability.













BOSTON PUBLIC LIBRARY



3 9999 06352 052 0



